

## Ex.No. 4

### Installation of rootkits and the study about various options

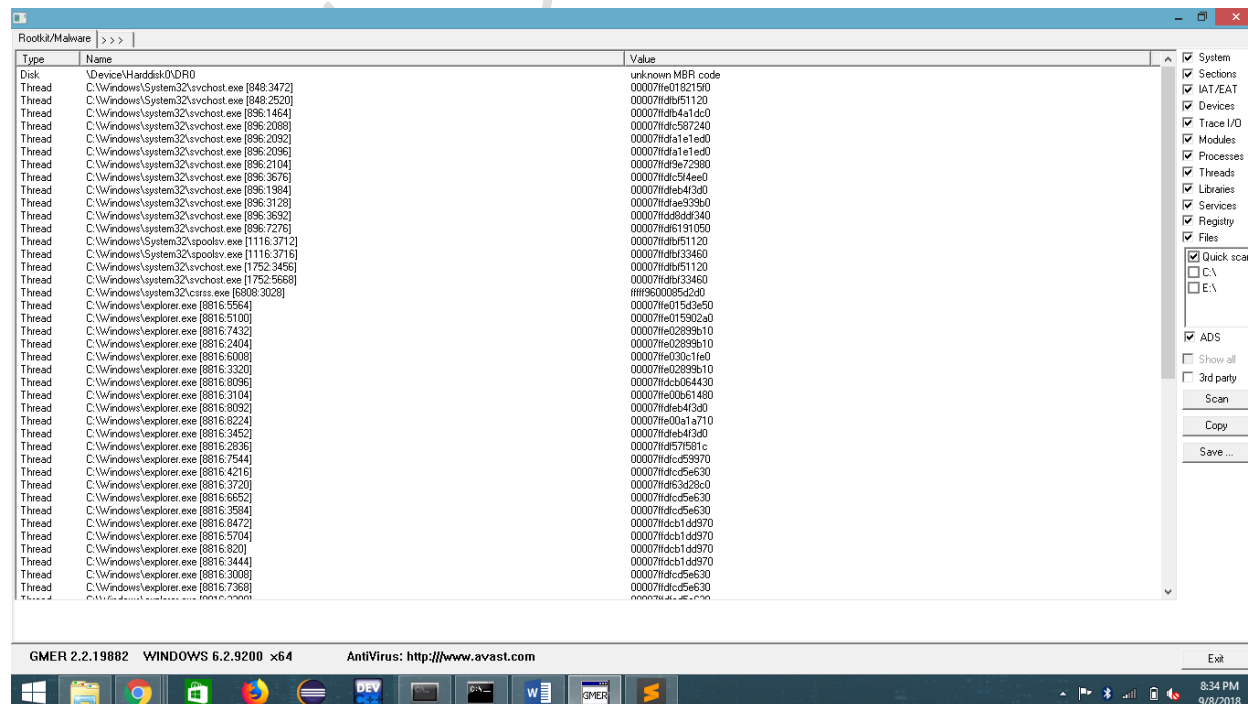
#### Aim:

To install rootkits and study the various options available.

#### Procedure:

1. Download the rootkit tool from the GMER website.
2. This tool displays the following options, Processes, Modules, Services, Files, Registry, Rootkit/Malware, Auto start, cmd of localhost.
3. Select Processes menu and kill any unwanted processes.
4. Modules menu display the various system files like .sys, .dll.
5. Services menu display the complete services running with Autostart, Enable, Disable, System, Boot.
6. Files menu display full files on hard-disk volumes.
7. Rootkits/Malware scans the local drivers selected.
8. Autostart displays the registry base Autostart applications.
9. CMD allows the user to interact with command line utilities or registry.

#### Output:





## Ex.No. 5

### Implement hacking windows – windows login and password

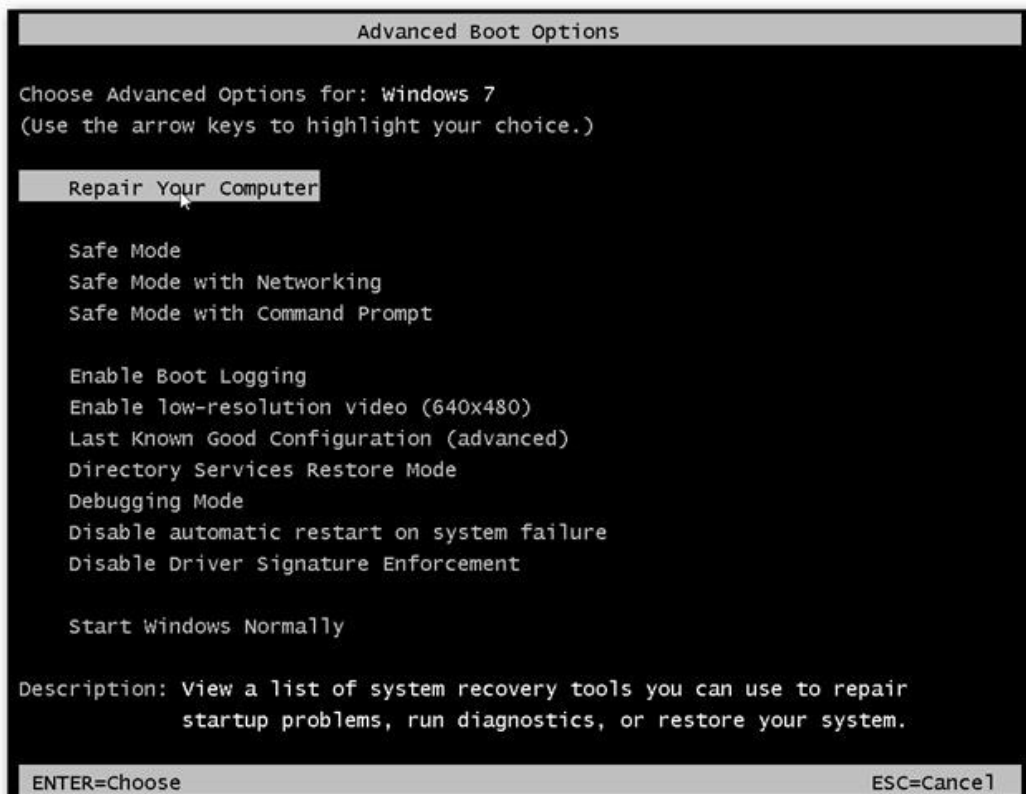
#### Aim:

To implement hacking windows to hack windows login and password.

#### Procedure:

1. Any Linux live CD/USB.
2. Insert the live CD/USB and boot from it.
3. Locate the driver where Windows is installed.
4. Rename the file named cmd.exe to cmd0.exe.
5. Rename the file named sethc.exe to cmd.exe.
6. Rename the file named cmd0.exe to sethc.exe.
7. Shut down and boot into windows.
8. Press shift key 5 times.
9. Type net user to display the list of active users.
10. Type net user <account name> \*.
11. It will ask for new password, enter the new password.
12. Done.

#### Output:





**Result:**

Thus hacking windows login and password has been implemented successfully.

## Ex.No.6

### Implement hacking windows – Accessing restricted drivers

#### Aim:

To implement hacking windows to access restricted drivers.

#### Procedure:

##### Task Manager

- If task manager can't be opened with the Ctrl-Alt-Delete shortcut, then you may want to try the Ctrl-Shift-Escape shortcut. It can open hundreds of error messages in a few seconds if this shortcut is blocked.
- There are other ways of opening Task Manager or similar tools. The blocked computers in most of the cases block both task manager shortcuts as well as installing and running new software, but they left Microsoft Access installed with full Visual Basic for Applications functionality, and many places on the Internet have codes for creating your own task manager or process list.

##### Remote Control

One way of opening a lot of blocked file formats or viewing blocked websites is by remotely controlling another machine that doesn't have these restrictions. One way is to use TeamViewer where you can install it on removable media, run it without installation on computers that stop you installing new software, or you can even use it through a web browser if you can't run .exe files.

##### Website Blocking

- The easiest way is to use a circumventor like stupidcensorship.com, although these are often blocked quite quickly as well, so sign up to their mailing list to receive emails whenever a new circumventing site is created.
- Check that the sites aren't blocked locally. Check this by going into your browser's "tools" section or its equivalent on whatever browser you use, click on security or a similar section and look for a restricted or blocked sites section, then view these sites and remove any you want to access if they're there.
- Accessing the blocked website using its IP address, you find this by opening the command prompt on any Windows computer (by typing cmd in the run box) and typing:

*ping www.example.com*

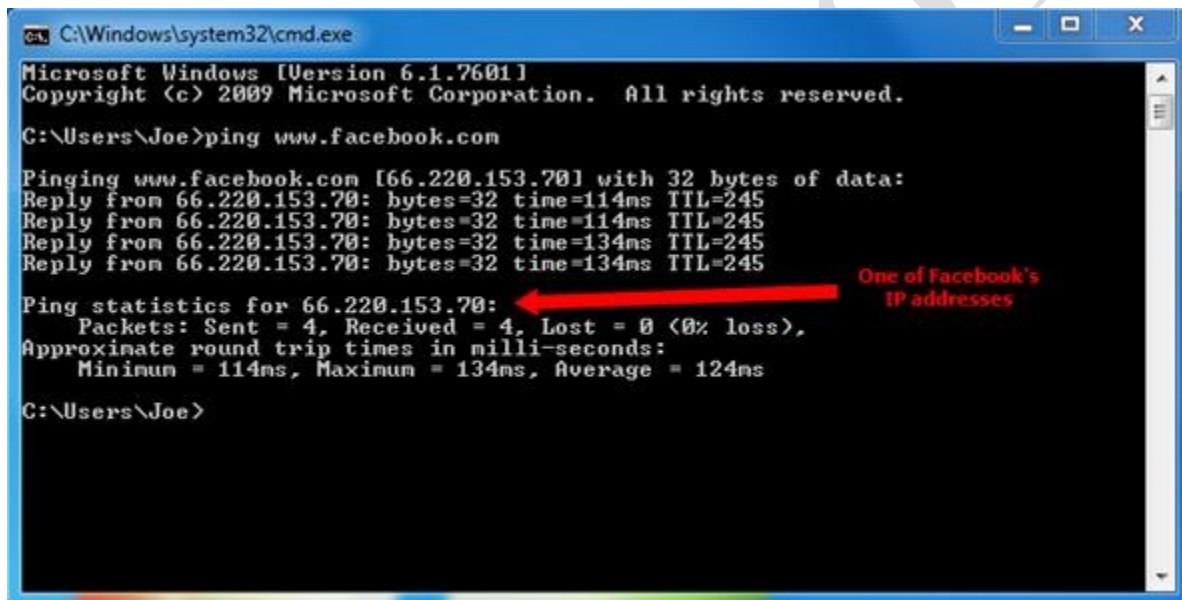
##### Installing Software

- There are several ways to find admin passwords, often the default passwords will still work, or you can use a password cracker like Ophcrack to find local admin passwords.
- If you have access to the command prompt on a Windows computer, then you can use the "Net user" and "Net Group" commands to find out details on each account, and if you know enough about command prompts, you may even be able to change the passwords.
- Boot Windows in safe mode by pressing F8 as Windows boots and trying to install the software then. Safe mode is a good way to bypass a lot of security software and restrictions. For example, my school had an "RM Login" screen that I could only skip by using safe mode.

## Running Software

- Using safe mode like in the last section, Use Notepad and make some kind of runnable file. Here is a list of some of the most common runnable formats on Windows: .exe, .bat, .vbs, .cmd
- Used is booting or running from an external device. I've used USB flash drives, CDs, DVDs and an external hard drive and have booted both Linux and Windows operating systems. Most operating systems can be installed on removable media. Once you've booted from this device, there are often no restrictions at all on the system other than Internet-based ones which force you to connect to the Internet through a proxy server that blocks websites, but like I've said, they're not hard to get around.

## Output:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Joe>ping www.facebook.com

Pinging www.facebook.com [66.220.153.70] with 32 bytes of data:
Reply from 66.220.153.70: bytes=32 time=114ms TTL=245
Reply from 66.220.153.70: bytes=32 time=114ms TTL=245
Reply from 66.220.153.70: bytes=32 time=134ms TTL=245
Reply from 66.220.153.70: bytes=32 time=134ms TTL=245

Ping statistics for 66.220.153.70:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 114ms, Maximum = 134ms, Average = 124ms

C:\Users\Joe>
```

A red arrow points from the text "One of Facebook's IP addresses" to the IP address 66.220.153.70 in the ping statistics.

## Result:

Thus accessing restricted drivers has been implemented successfully.