Date: 03/01 /25

Lab Practical #4:

Perform Steganography and DOS attack.

1. Steganography using steghide:
   - Install Steghide using apt as shown below and enter your password:

```
┌──(mudit㉿kali)-[~/Desktop/DOS]
└─$ sudo apt install steghide
The following packages were automatically installed and are no longer required:
  chrome-gnome-shell        libgspell-1-2      libwinpr2-2t64
  fonts-liberation2         libibverbs1        libzip4t64
  freerdp2-x11              libimobiledevice6  perl-modules-5.38
```

   - Now to actually hide a file in a image we will do the following command.

```
┌──(mudit㉿kali)-[~/Desktop/DOS]
└─$ cat Steg.txt
Perform Steganography and DOS attack
```

   - The below command contains following parameters & flags: ◦
     - embed: Embed secret data in a cover file thereby creating a stego file.
     - ◦-ef (Shorthand for –-embedfile): Specify the file that will be embedded (the file that contains the secret message). Note that steghide embeds the original file name in the stego file. When extracting data (see below) the default behaviour is to save the embedded file into the current directory under its original name. If this argument is omitted or filename is -, steghide will read the secret data from standard input. In our case the file name is “file.txt”
     - ◦-cf (Shorthand for –coverfile): Specify the cover file that will be used to embed data. The cover file must be in one of the following formats: AU, BMP, JPEG or WAV. The file-format will be detected automatically based on header information (the extension is not relevant). If this argument is omitted or filename is -, steghide will read the cover file from standard input. In our case the name is “image.jpeg”.

```
┌──(mudit㉿kali)-[~/Desktop/DOS]
└─$ steghide embed -ef Steg.txt -cf Kali_new.jpeg
Enter passphrase:
Re-Enter passphrase:
embedding "Steg.txt" in "Kali_new.jpeg"... done
```

Date: 03/01 /25

- Now to extract the hidden data from the file we will use the following command:

```
┌──(mudit㉿kali)-[~/Desktop/DOS]
└─$ steghide extract -sf ./Kali_new.jpeg -xf ./img.txt
Enter passphrase:
the file "./img.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "./img.txt".
```

  - The above command contains following parameters & flags:
    - extract: Extract secret data from a stego file.
    - -sf (Shorthand for -–stegofile): Specify the name for the stego file that will be created. If this argument is omitted when calling steghide with the embed command, then the modifications to embed the secret data will be made directly to the cover file without saving it under a new name. In our case it will be “image.jpeg”
    - -xf (Shorthand for –extractfile): Create a file with the name filename and write the data that is embedded in the stego file to it. This option overrides the filename that is embedded int the stego f ile. If this argument is omitted, the embedded data will be saved to the current directory under its original name. In our case it will be “data.txt”.

2. DOS Attack:

  - hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. hping3 handle fragmentation, arbitrary packets body and size and can be used in order to transfer files encapsulated under supported protocols. Using hping3 you are able to perform at least the following stuff:

    - Test firewall rules.
    - Perform advanced port scanning.
    - Test network performance using:
    - Different protocols.
    - Various sizes, TOS (Type of Service), and fragmentation.
    - Conduct Path MTU (Maximum Transmission Unit) discovery.
    - Transfer files even through strict firewall rules.
    - Perform traceroute-like analysis under different protocols.
    - Utilize Firewalk-like capabilities.
    - Perform remote OS fingerprinting.
    - Audit TCP/IP stacks.
    - Execute various other advanced network-related tasks.

Date: 03/01 /25

To perfrom DOS (Denial Of Service) attack we will use the following command:

- sudo hping3 -S -p <port_no> -d <data_size> <ip_address> –flood

```
┌──(mudit㉿kali)-[~/Desktop/DOS]
└─$ sudo hping3 -S -p 80 -d 1200 103.13.112.180 --flood
HPING 103.13.112.180 (eth0 103.13.112.180): S set, 40 headers + 1200 data bytes
hping in flood mode, no replies will be shown
```

- the above command is explained below:
  - **`sudo`**:
    - Allows a permitted user to execute a command as the superuser.
  - **`-S` (SYN Flag)**:
    - Tells `hping3` to send a TCP SYN packet to the target.
    - Used to launch a SYN flood attack.
  - **`-p` (Destination Port)**:
    - Shorthand for `--destport`.
    - Sets the destination port; the default is 0.
    - If preceded by a `+` (e.g., `+1024`), the destination port increases for each reply received.
    - In this case: `-p 80` targets HTTP.
  - **`-d` (Packet Body Size)**:
    - Sets the packet body size in bytes.
    - Example: `-d 1200000` sets the packet size to 1,200,000 bytes.
  - **`--flood` (Flood Mode)**:
    - Sends packets as fast as possible without showing incoming replies.
    - Much faster than specifying the `-i u0` option.