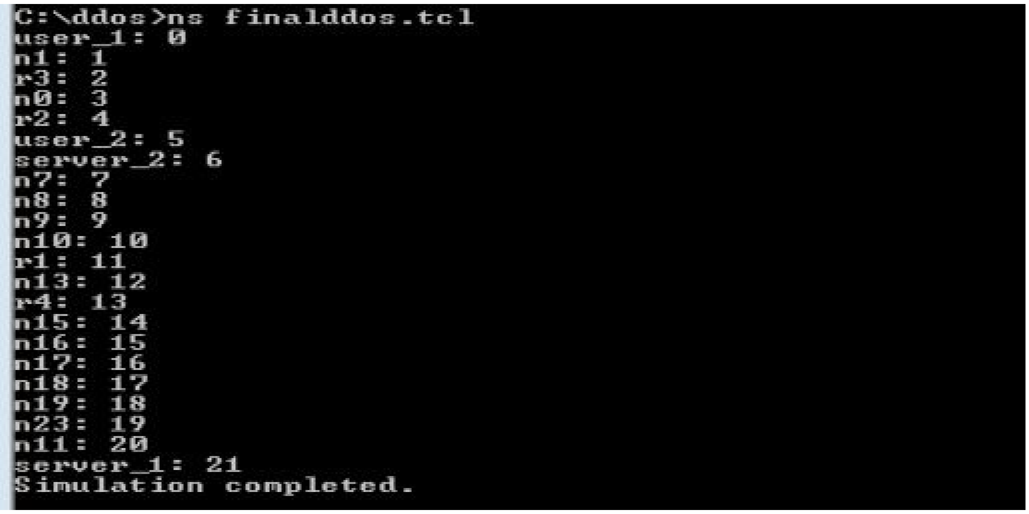
Parag Mhatre
ITIS 6167

In this scenario, user 2 is trying to reach server 1 and user 1 is trying to reach server 2.

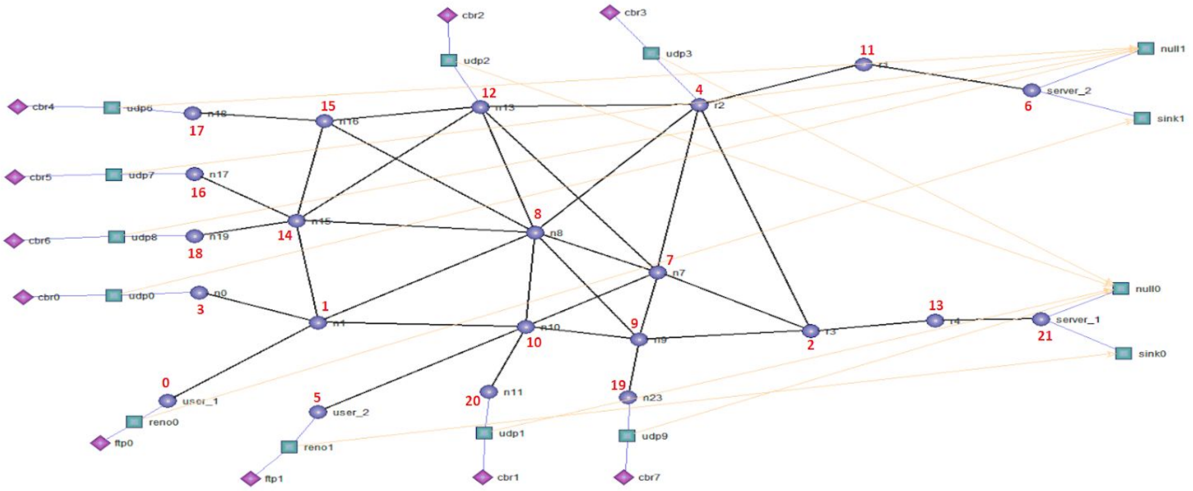
Source (attacker)	**Destination**	**Traffic rate (KB per second)**
cbr0	server_2	512 kb/s
cbr4	server_2	512 kb/s
cbr5	server_2	512 kb/s
cbr6	server_2	512 kb/s
cbr2	server_1	512 kb/s
cbr3	server_1	512 kb/s
cbr1	server_1	512 kb/s
cbr7	server_1	512 kb/s
8 bots		**4096 kb/s**

The node to number mapping is as follows:



```
C:\ddos>ns finalddos.tcl
user_1: 0
n1: 1
r3: 2
n0: 3
r2: 4
user_2: 5
server_2: 6
n7: 7
n8: 8
n9: 9
n10: 10
r1: 11
n13: 12
r4: 13
n15: 14
n16: 15
n17: 16
n18: 17
n19: 18
n23: 19
n11: 20
server_1: 21
Simulation completed.
```

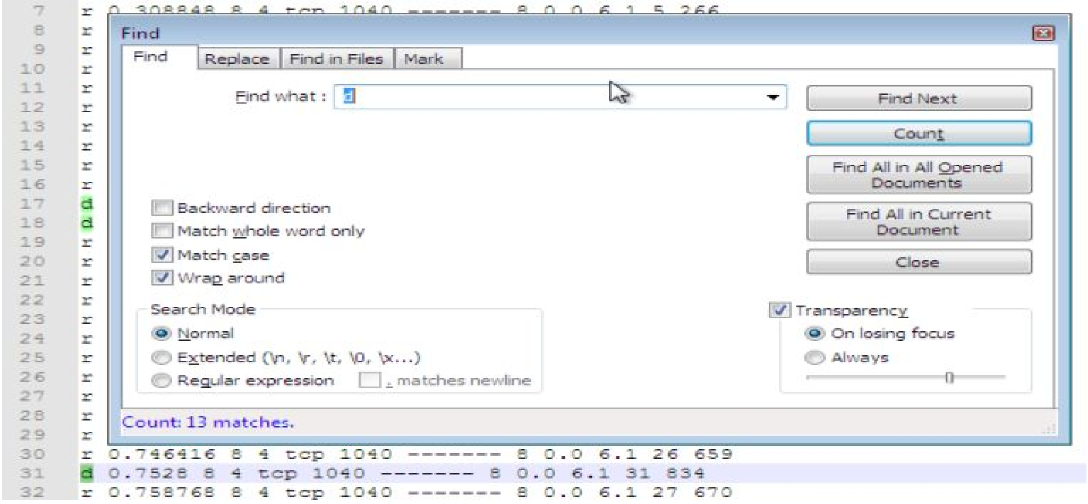
The network design is:



For user 1 and server 2:

- The link connecting n8(8) and r2(4) is congested.
- I noticed 153 reads and 13 drops between n8 and r2.
- I used Powershell commands like

```
“type finalddos.tr | Select-String "0.0 6.1" | Select-String " 8 4 " |
Select-String "r |d " | Out-File user1.txt”
```



```
r 0.308848 8 4 tcp 1040 ------- 8 0.0 6.1 5 266
r
r
r
r
r
r
r
r
r
d
d
r
r
r
r
r
r
r
r
r
r
r
r 0.746416 8 4 tcp 1040 ------- 8 0.0 6.1 26 659
d 0.7528 8 4 tcp 1040 ------- 8 0.0 6.1 31 834
r 0.758768 8 4 tcp 1040 ------- 8 0.0 6.1 27 670
```

Find

Find what : d

☐ Backward direction
☐ Match whole word only
☑ Match case
☑ Wrap around

Search Mode
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression ☐ . matches newline

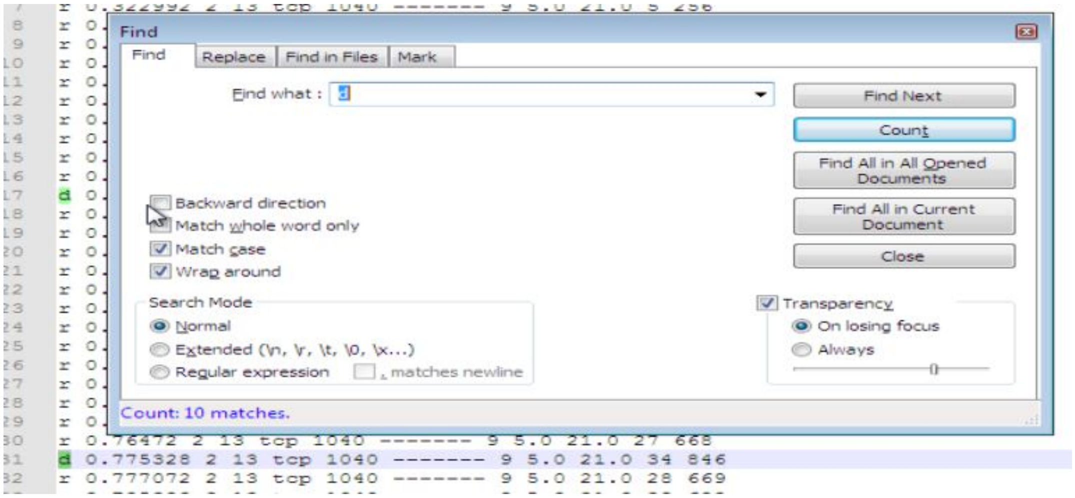
☑ Transparency
● On losing focus
○ Always

Count: 13 matches.

Find
Replace
Find in Files
Mark
Find Next
Count
Find All in All Opened Documents
Find All in Current Document
Close

For user 2 and server 1:

- The link connecting r3(2) and r4(13) is congested.
- I noticed 183 reads and 10 drops between r3 and r4.



```
r 0.322992 2 13 tcp 1040 ------- 9 5.0 21.0 5 256
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.
d 0.
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.
r 0.76472 2 13 tcp 1040 ------- 9 5.0 21.0 27 668
d 0.775328 2 13 tcp 1040 ------- 9 5.0 21.0 34 846
r 0.777072 2 13 tcp 1040 ------- 9 5.0 21.0 28 669
```

Find

Find what : d

□ Backward direction
□ Match whole word only
☑ Match case
☑ Wrap around

Search Mode
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression □ . matches newline

☑ Transparency
● On losing focus
○ Always

Count: 10 matches.

Find
Replace
Find in Files
Mark
Find Next
Count
Find All in All Opened Documents
Find All in Current Document
Close

Summary:

The Crossfire attack is a type of Denial of Service attack aimed at disrupting communication from node A to node B. An attacker can deploy an army of bots to target a bottleneck node which is crucial for the communication path to exist for node A and node B to be able to communicate. The important task here is the identification of the target node which is vulnerable to such an attack and is crucial for the communication path to work at the same time. This type of attack is also difficult to detect as multiple attack nodes send low intensity traffic flows to the target nodes. These are very similar to legitimate traffic flows. In this attack, the target server has no knowledge of the attack as the attack actually happens on an arbitrary node which in turn results in the traffic flow cut-off between two legitimate nodes.

There has been a good amount of research on how to defend against this attack and some possible solutions involve Artificial Intelligence based, Data analysis based solutions. I feel that an IDS can also defend against crude versions of such attacks using deep packet inspection. There was a solution suggested in one of the papers that had a monitoring system which monitors for congestion and remedies the situation based on the scenario. Similarly, SDN can also play some part in alleviating this attack as it has global view and can easily assign a different route for packets if a certain route is congested.

Sources:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.736.6090&rep=rep1&type=pdf
https://www.ieee-security.org/TC/SP2013/papers/4977a127.pdf