## Denial of Service (DoS) Attack - Hping3, METASPLOIT:

```
alert ip any any -> any any (msg:"DoS Attack detected - SYN Flood"; flags:S; detection_filter: track by_src, count 100, seconds 10; sid:2000001;)

alert ip any any -> any any (msg:"DoS Attack detected - UDP Flood"; flow:stateless; detection_filter: track by_src, count 200, seconds 10; sid:2000002;)

alert ip any any -> any any (msg:"DoS Attack detected - ICMP Flood"; icmp_type:8; detection_filter: track by_src, count 300, seconds 10; sid:2000003;)

alert tcp any any -> any any (msg:"DoS Attack detected - RST Flood"; flags:R; detection_filter: track by_src, count 100, seconds 10; sid:2000004;)

alert tcp any any -> any any (msg:"DoS Attack detected - FIN Flood"; flags:F; detection_filter: track by_src, count 100, seconds 10; sid:2000005;)

alert ip any any -> any any (msg:"DoS Attack detected - HTTP GET Flood"; content:"GET "; http_method; detection_filter: track by_src, count 500, seconds 10; sid:2000006;)

alert ip any any -> any any (msg:"DoS Attack detected - HTTP POST Flood"; content:"POST "; http_method; detection_filter: track by_src, count 500, seconds 10; sid:2000007;)

alert ip any any -> any any (msg:"DoS Attack detected - Slowloris Attack"; flow:established; content:"User-Agent"; http_header; detection_filter: track by_src, count 10, seconds 60; sid:2000008;)

alert tcp any any -> any any (msg:"DoS Attack detected - Connection Exhaustion"; flags:S; threshold:type threshold, track by_dst, count 1000, seconds 10; sid:2000009;)

alert ip any any -> any any (msg:"DoS Attack detected - DNS Amplification"; content:"\x00\x01\x00\x00\x00\x00"; offset:2; depth:6; sid:2000010;)

alert tcp any any -> any any (msg:"DoS Attack detected - Large Payload SYN Flood"; flags:S; dsize:>1000; sid:2000021;)

alert tcp any any -> any any (msg:"DoS Attack detected - Malformed TCP Header"; content:"\x00\x00\x00\x00"; offset:12; depth:4; sid:2000022;)

alert ip any any -> any any (msg:"DoS Attack detected - ICMP Fragmentation Attack"; icmp_type:3; dsize:<100; sid:2000023;)
alert ip any any -> any any (msg:"DoS Attack detected - Fake ICMP
Timestamp Requests"; icmp_type:13; sid:2000024;)

alert tcp any any -> any any (msg:"DoS Attack detected - Multiple
Simultaneous Connections"; detection_filter: track by_src, count 500, seconds
10; sid:2000025;)

alert ip any any -> any any (msg:"DoS Attack detected - High Volume DNS
Queries"; dns_query; detection_filter: track by_src, count 200, seconds 10;
sid:2000026;)

alert tcp any any -> any any (msg:"DoS Attack detected - Large TCP
Retransmissions"; detection_filter: track by_src, count 400, seconds 20;
sid:2000027;)

alert ip any any -> any any (msg:"DoS Attack detected - Repeated HTTP 503
Responses"; http_status; content:"503"; detection_filter: track by_src, count 50,
seconds 10; sid:2000028;)

alert tcp any any -> any any (msg:"DoS Attack detected - Excessive SSL
Handshakes"; tls.handshake_type; content:"\x01"; detection_filter: track
by_src, count 100, seconds 10; sid:2000029;)

alert ip any any -> any any (msg:"DoS Attack detected - Unusually High
Connection Attempts"; detection_filter: track by_src, count 1000, seconds 30;
sid:2000030;)

alert ip any any -> any any (msg:"DoS Attack detected - SIP INVITE Flood";
content:"INVITE"; sip_method; detection_filter: track by_src, count 200,
seconds 10; sid:2000031;)

alert ip any any -> any any (msg:"DoS Attack detected - SMTP Connection
Flood"; content:"EHLO"; smtp_command; detection_filter: track by_src, count
300, seconds 10; sid:2000032;)

alert ip any any -> any any (msg:"DoS Attack detected - Excessive FTP
Connection Requests"; content:"USER"; ftp_command; detection_filter: track
by_src, count 150, seconds 10; sid:2000033;)

alert ip any any -> any any (msg:"DoS Attack detected - Repeated RDP
Connection Attempts"; content:"Cookie:"; detection_filter: track by_src, count
200, seconds 10; sid:2000034;)

alert ip any any -> any any (msg:"DoS Attack detected - Large Volume of NTP
Monlist Requests"; content:"monlist"; ntp_request; detection_filter: track
by_src, count 100, seconds 10; sid:2000035;)
```

```
alert tcp any any -> any any (msg:"DoS Attack detected - Excessive TCP Connection Resets"; flags:R; detection_filter: track by_src, count 500, seconds 10; sid:2000036;)

alert ip any any -> any any (msg:"DoS Attack detected - Sudden Increase in ICMP Traffic"; icmp_type:8; detection_filter: track by_src, count 500, seconds 10; sid:2000037;)

alert ip any any -> any any (msg:"DoS Attack detected - Malformed UDP Packets"; dsize:>1200; sid:2000038;)

alert ip any any -> any any (msg:"DoS Attack detected - Excessive SSH Login Attempts"; content:"SSH-2.0"; detection_filter: track by_src, count 200, seconds 10; sid:2000039;)

alert ip any any -> any any (msg:"DoS Attack detected - High Volume of DNS TXT Queries"; dns_query; content:"TXT"; detection_filter: track by_src, count 150, seconds 10; sid:2000040;)
```