**Tool- MHDDoS - DDoS Attack Script With 56 Methods**

**Features And Methods**

* 💣 Layer7
  + [get](https://camo.githubusercontent.com/1de6b02ca58ff0ac5f9a7d0993b689e7fb5d7f516615c6f846b928857bb0a13e/68747470733a2f2f696d672e69636f6e73382e636f6d2f636f74746f6e2f3334342f646f6d61696e2e706e67) GET | GET Flood
  + [post](https://camo.githubusercontent.com/b17c7f5f9261c16b21d15e3d2865f90e84ce3456dfd367a789cbca765e5a3fba/68747470733a2f2f63646e302e69636f6e66696e6465722e636f6d2f646174612f69636f6e732f64617461626173652d73746f726167652d352f36302f7365727665725f5f64617461626173655f5f666972655f5f6275726e5f5f7361666574792d3531322e706e67) POST | POST Flood
  + [ovh](https://camo.githubusercontent.com/0329100ee05143dd0cd08c6ba2cb18b4e75ee495a2c589c44e1364c8071b97c1/68747470733a2f2f7374617469632d30302e69636f6e6475636b2e636f6d2f6173736574732e30302f6f76682d69636f6e2d3230343878323034382d6c346333697a76672e706e67) OVH | Bypass OVH
  + [ovh](https://camo.githubusercontent.com/e2c6d236c6259b9c18922b43834a99f810b4c7aa31e5fd807432a41f947598e5/68747470733a2f2f63646e2d69636f6e732d706e672e666c617469636f6e2e636f6d2f3531322f313639312f313639313934382e706e67) RHEX | Random HEX
  + [ovh](https://camo.githubusercontent.com/514519cd049f404da3d47a818dad5b15ed0cd00e90089b49fc1ba212af46e109/68747470733a2f2f63646e2d69636f6e732d706e672e666c617469636f6e2e636f6d2f3531322f343333372f343333373937322e706e67) STOMP | Bypass chk\_captcha
  + [stress](https://camo.githubusercontent.com/117ceb25f317a6deeea78e54a58cdd01c752b8b1e4a3c031d9f3f2ef6cb18760/68747470733a2f2f63646e2e69636f6e73636f75742e636f6d2f69636f6e2f7072656d69756d2f706e672d3235362d7468756d622f63796265722d62756c6c79696e672d323535373739372d323135323337312e706e67) STRESS | Send HTTP Packet With High Byte
  + [dyn](https://camo.githubusercontent.com/e6a1bc91b2ce244cee597cd10cf00a2b341b82ddb252c0d0d6ac89ca03de0d9e/68747470733a2f2f7062732e7477696d672e636f6d2f70726f66696c655f696d616765732f313335313536323938373232343634313534342f494b6234715f79645f343030783430302e6a7067) DYN | A New Method With Random SubDomain
  + [downloader](https://camo.githubusercontent.com/88bc42d4f7adea80d9db05fdaec38c7e8673cbb5c5435090c77567e5e61d0b4e/68747470733a2f2f63646e2d69636f6e732d706e672e666c617469636f6e2e636f6d2f3531322f363939312f363939313634332e706e67) DOWNLOADER | A New Method of Reading data slowly
  + [slow](https://camo.githubusercontent.com/4473d3cd657e0a3b126ff50154ebdd0a8e95ddfb8cd2599e80443cf1b171d643/68747470733a2f2f63646e322e69636f6e66696e6465722e636f6d2f646174612f69636f6e732f706f69736f6e2d616e642d76656e6f6d2d66696c6c2f3136302f6c6f726973322d3531322e706e67) SLOW | Slowloris Old Method of DDoS
  + [head](https://camo.githubusercontent.com/4a01a6a33f5ad5fb309181b9103494132eb30dc7d6755d9fe0bdcff7ee44a876/68747470733a2f2f6c797261686f7374696e672e636f6d2f77702d636f6e74656e742f75706c6f6164732f323032302f30362f64646f732d686f772d776f726b2d69636f6e2e706e67) HEAD | <https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/HEAD>
  + [null](https://camo.githubusercontent.com/90a4d818b8113dfd424de180659ad1a4ebfef737d67453db2a01583301d3fd5c/68747470733a2f2f696d672e69636f6e73382e636f6d2f706c6173746963696e652f32782f6e756c6c2d73796d626f6c2e706e67) NULL | Null UserAgent and ...
  + [cookie](https://camo.githubusercontent.com/a94b4c67e47993ff4e141f867fbad9d87f599e02183241beaa0b3873d9e8517b/68747470733a2f2f692e70696e696d672e636f6d2f6f726967696e616c732f30332f32652f37642f30333265376430373535636435313163373533626362363033356434346636382e706e67) COOKIE | Random Cookie PHP 'if (isset($\_COOKIE))'
  + [pps](https://camo.githubusercontent.com/1228b910d405c2f117640fb41bc93a79b9984b39c7719a60a0ed98e4151ed6ec/68747470733a2f2f63646e302e69636f6e66696e6465722e636f6d2f646174612f69636f6e732f6469637469636f6e732d66696c65732d666f6c646572732f33322f6f66666963655f7070732d3531322e706e67) PPS | Only 'GET / HTTP/1.1\r\n\r\n'
  + [even](https://camo.githubusercontent.com/82b10990accda48cd8695fe14ac99eab5764e663cbc2063721459f690c59a195/68747470733a2f2f63646e332e69636f6e66696e6465722e636f6d2f646174612f69636f6e732f696e7465726e65742d73656375726974792d31342f34382f44446f535f776562736974655f776562706167655f626f6d625f76697275735f70726f74656374696f6e2d3531322e706e67) EVEN | GET Method with more header
  + [googleshield](https://camo.githubusercontent.com/04e4fbe63d94ed12610abbae074c0ee5ee1af1a311610f7d7dbf3c712b6068ae/68747470733a2f2f69696c692e696f2f485539424337342e706e67) GSB | Google Project Shield Bypass
  + [](https://camo.githubusercontent.com/a4e3b4cde57f1c5e16f6abad5623c52ae883d2446357a4f82d1ad9df6f04c3aa/68747470733a2f2f7365656b6c6f676f2e636f6d2f696d616765732f442f64646f732d67756172642d6c6f676f2d434645464341343039432d7365656b6c6f676f2e636f6d2e706e67) DGB | DDoS Guard Bypass
  + [ArvanCloud](https://camo.githubusercontent.com/3790a327f2ac8f2f8edbd234cc4a35d7bd05fb4ab441278c7d8e21141f84fb1a/68747470733a2f2f692e696d6775722e636f6d2f62474c387166772e706e67) AVB | Arvan Cloud Bypass
  + [Google bot](https://camo.githubusercontent.com/04e4fbe63d94ed12610abbae074c0ee5ee1af1a311610f7d7dbf3c712b6068ae/68747470733a2f2f69696c692e696f2f485539424337342e706e67) BOT | Like Google bot
  + [Apache Webserver](https://camo.githubusercontent.com/97044d35a8581a916b6360576404adc3ad9eeb7cb4a0fc0b7ce64f8a8d202d21/68747470733a2f2f75706c6f61642e77696b696d656469612e6f72672f77696b6970656469612f636f6d6d6f6e732f7468756d622f612f61382f4170616368655f485454505f5365727665725f4c6f676f5f253238323031362532392e7376672f3130303070782d4170616368655f485454505f5365727665725f4c6f676f5f253238323031362532392e7376672e706e67) APACHE | Apache Expliot
  + [](https://camo.githubusercontent.com/69f9af595bfe8049d4ccf104efd9ca07a0ff7cc5ccf5f845feb67dde8ba6134b/68747470733a2f2f69636f6e2d6c6962726172792e636f6d2f696d616765732f69636f6e2d666f722d776f726470726573732f69636f6e2d666f722d776f726470726573732d31362e6a7067) XMLRPC | WP XMLRPC exploit (add /xmlrpc.php)
  + [](https://camo.githubusercontent.com/332477585898727a1947cbdbfd87afe7e429ab47e7f31c774c5460a86919a8f7/68747470733a2f2f746563686372756e63682e636f6d2f77702d636f6e74656e742f75706c6f6164732f323031392f30362f4a324c6c48715433714a6c30624739416c7067632d312d373330783433382e706e673f773d373330) CFB | CloudFlare Bypass
  + [](https://camo.githubusercontent.com/332477585898727a1947cbdbfd87afe7e429ab47e7f31c774c5460a86919a8f7/68747470733a2f2f746563686372756e63682e636f6d2f77702d636f6e74656e742f75706c6f6164732f323031392f30362f4a324c6c48715433714a6c30624739416c7067632d312d373330783433382e706e673f773d373330) CFBUAM | CloudFlare Under Attack Mode Bypass
  + BYPASS | Bypass Normal AntiDDoS
  + [bypass](https://camo.githubusercontent.com/e7ec74926910c2ddc06301ab4aafe115f1cbd86a34a63fadf56612080ac6e088/68747470733a2f2f63646e2d69636f6e732d706e672e666c617469636f6e2e636f6d2f3531322f3930352f3930353536382e706e67) BOMB | Bypass with codesenberg/bombardier
  + 🔪 KILLER | Run many threads to kill a target
  + 🧅 TOR | Bypass onion website
* 🧨 Layer4:
  + [tcp](https://raw.githubusercontent.com/kgretzky/pwndrop/master/media/pwndrop-logo-512.png) TCP | TCP Flood Bypass
  + [](https://camo.githubusercontent.com/2eec5ca76c62b2456cb89c0a4d214871dc6f9e5b052d171c50aa5fce6815be5e/68747470733a2f2f7374796c65732e7265646469746d656469612e636f6d2f74355f3272786d69712f7374796c65732f70726f66696c6549636f6e5f736e6f6f62393463646230392d633236632d346332342d626430632d3636323338363233636332322d6865616473686f742e706e67) UDP | UDP Flood Bypass
  + [syn](https://camo.githubusercontent.com/e9d0fd0240b783e3c73dd7c4d6ed40fd8bb28c24ad3de85d8e9d0759a9e8b288/68747470733a2f2f63646e2d69636f6e732d706e672e666c617469636f6e2e636f6d2f3531322f313931382f313931383537362e706e67) SYN | SYN Flood
  + [cps](https://camo.githubusercontent.com/5db4e8430a3836e1e476e08f66b415bec4df8a226e3154a713380a345f782d91/68747470733a2f2f63646e2d69636f6e732d706e672e666c617469636f6e2e636f6d2f3531322f313031372f313031373436362e706e67) CPS | Open and close connections with proxy
  + [icmp](https://camo.githubusercontent.com/3f7c8ffdf0f4d9c874b556ea76f39293d3ef2acae467d8ab664d8b4bc7f13812/68747470733a2f2f69636f6e2d6c6962726172792e636f6d2f696d616765732f69636f6e2d70696e672f69636f6e2d70696e672d32382e6a7067) ICMP | Icmp echo request flood (Layer3)
  + [connection](https://camo.githubusercontent.com/071beae45b4459cf8e22b7058f9c9a9c5d638fcc626559d476317f57b07988bb/68747470733a2f2f73362e7575706c6f61642e69722f66696c65732f313035393634335f673868702e706e67) CONNECTION | Open connection alive with proxy
  + [vse](https://camo.githubusercontent.com/33803aa624a3f48fec0623ee8ee14bebfd2092660bb3994820b84fb127139ade/68747470733a2f2f69613830333130392e75732e617263686976652e6f72672f32372f6974656d732f736f757263652d656e67696e652d766964656f2d70726f6a656374732f736f757263652d656e67696e652d766964656f2d70726f6a656374735f6974656d696d6167652e706e67) VSE | Send Valve Source Engine Protocol
  + [teamspeak 3](https://camo.githubusercontent.com/df97f8ef28d03075a378c741e9f5f58636473ca9e0c2cf95e184f01db1d0f083/68747470733a2f2f6d79637261636b667265652e636f6d2f77702d636f6e74656e742f75706c6f6164732f323031382f30382f5465616d537065616b2d5365727665722d392e706e67) TS3 | Send Teamspeak 3 Status Ping Protocol
  + [fivem](https://camo.githubusercontent.com/3c80ec89808b5c622211252a00682a126f3468106b9d73b6e48bf8b53db10cd9/68747470733a2f2f63646e322e646f776e6465746563746f722e636f6d2f7374617469632f75706c6f6164732f6c6f676f2f373565663966636162633161626561386663653065626430323336613431333237313066636232652e706e67) FIVEM | Send FiveM Status Ping Protocol
  + [mem](https://camo.githubusercontent.com/3af54b50d6db9601933997e395fa73efe19b09fc9397fc057d681e586f64cba5/68747470733a2f2f63646e2e69636f6e73636f75742e636f6d2f69636f6e2f667265652f706e672d3531322f72656469732d342d313137353130332e706e67) MEM | Memcached Amplification
  + [ntp](https://camo.githubusercontent.com/2b62fca93e48bf9c3e2d390e483ac801039436f2939e14089c9ddaa5ba0c766a/68747470733a2f2f6c797261686f7374696e672e636f6d2f77702d636f6e74656e742f75706c6f6164732f323032302f30362f64646f732d61747461636b2d69636f6e2e706e67) NTP | NTP Amplification
  + [mcbot](https://camo.githubusercontent.com/192598ba1b8cfd8b27d038358fbbe474d41da20398d4fc288d1e978cde1eb9b5/68747470733a2f2f63646e2d69636f6e732d706e672e666c617469636f6e2e636f6d2f3531322f343731322f343731323133392e706e67) MCBOT | Minecraft Bot Attack
  + [minecraft](https://camo.githubusercontent.com/8f88954d654d3c9a87b0f606df6c8420d0ea9a929a501279fbe04678cfe911cf/68747470733a2f2f63646e2e69636f6e2d69636f6e732e636f6d2f69636f6e73322f323639392f504e472f3531322f6d696e6563726166745f6c6f676f5f69636f6e5f3136383937342e706e67) MINECRAFT | Minecraft Status Ping Protocol
  + [minecraft pe](https://camo.githubusercontent.com/8f88954d654d3c9a87b0f606df6c8420d0ea9a929a501279fbe04678cfe911cf/68747470733a2f2f63646e2e69636f6e2d69636f6e732e636f6d2f69636f6e73322f323639392f504e472f3531322f6d696e6563726166745f6c6f676f5f69636f6e5f3136383937342e706e67) MCPE | Minecraft PE Status Ping Protocol
  + [dns](https://camo.githubusercontent.com/cf2c138e918b795bab3c394881ad5b3ff16a64cb713579693bb62758d1be7608/68747470733a2f2f63646e2d69636f6e732d706e672e666c617469636f6e2e636f6d2f3531322f323635332f323635333436312e706e67) DNS | DNS Amplification
  + [chargen](https://camo.githubusercontent.com/2b62fca93e48bf9c3e2d390e483ac801039436f2939e14089c9ddaa5ba0c766a/68747470733a2f2f6c797261686f7374696e672e636f6d2f77702d636f6e74656e742f75706c6f6164732f323032302f30362f64646f732d61747461636b2d69636f6e2e706e67) CHAR | Chargen Amplification
  + [](https://camo.githubusercontent.com/f5ec772dd1ec3cf1b22d60a6af2b6fef4e0bdacd6145476f63545449ddf0afeb/68747470733a2f2f656e637279707465642d74626e302e677374617469632e636f6d2f696d616765733f713d74626e3a414e64394763526374354f766a53437055667479524d6d3365766764504f612d66384c62774a464f2d4126757371703d434155) CLDAP | Cldap Amplification
  + [ard](https://camo.githubusercontent.com/e77f0bba6365073cc91210f9e873bbc46f0932e4c8a1e5d5eb26995c68998741/68747470733a2f2f68656c702e6170706c652e636f6d2f6173736574732f3631373142443243353838453532363231383234343039442f3631373142443244353838453532363231383234343041342f656e5f55532f38623633313335336530373034323066343735333062663935663161376661652e706e67) ARD | Apple Remote Desktop Amplification
  + [rdp](https://camo.githubusercontent.com/4347be2e2a00af4a436557eb12c624cc32c4f1e2e1ef94ce9a50071b8a185c13/68747470733a2f2f7777772e74656e666f72756d732e636f6d2f6765656b2f676172732f696d616765732f322f74797065732f7468756d625f5f656d6f74655f5f65736b746f705f5f6f6e6e656374696f6e2e706e67) RDP | Remote Desktop Protocol Amplification
* ⚙️ Tools - Runs With python3 start.py tools
  + 🌟 CFIP | Find Real IP Address Of Websites Powered By Cloudflare
  + 🔪 DNS | Show DNS Records Of Sites
  + 📍 TSSRV | TeamSpeak SRV Resolver
  + ⚠ PING | PING Servers
  + 📌 CHECK | Check If Websites Status
  + 😎 DSTAT | That Shows Bytes Received, bytes Sent and their amount
* 🎩 Other
  + ❌ STOP | STOP All Attacks
  + 🌠 TOOLS | Console Tools
  + 👑 HELP | Show Usage Script