**HTTP POST Flood**

קיים קושי בהבדלה בין תעבורה חוקית להתקפה המנגון היעיל ביותר שקיים היום הוא ע"י שילוב של שיטות אפיון תנועת הבקשות וכן זיהוי איפי משתמש המקור.

בשימוש ב יו אר אל רנדומלי ננסה לאחר הבנה שההתקפה הייתה מסוג זה כברירת מחדל לבצע בדיקת חריגות ונחסום אותם עם חומת האש. חלק מבדיקת החריגות היא לנסות לזהות את משתמש המקור שמפעיל את ההתקפה ניתן לשים לב לפעמים כי יש חלק מחתימת החבילות זהה כמו גודל החבילות

**SSL FLOOD**

using the BIG-IP system and the F5 iRules scripting language.

Now available via the F5 DevCentral online community, this iRule states that if a device tries to renegotiate more than five times in any 60-second period, the connection is silently dropped.

The biggest benefit to this approach is that the attacker believes the attack is still working and in service, when in actuality, the server has ignored the request and moved on to processing valid user requests instead.

**HTTP GET FLOOD**

today We know about two detection algorithms, one is focusing on a browsing order of pages and the other is focusing on a correlation with browsing time to page information size. that implement detection techniques and evaluate attack detection rates, i.e., false positive and false negative. The results show that our techniques can detect the HTTP-GET flood attack effectively.

**SYN FLOOD**

We have a lot of solution for this attack:

Filtering ,Increasing Backlog,Reducing SYN-RECEIVED Timer,Recycling the Oldest Half-Open TCP,SYN Cache,SYN cookies,Hybrid Approaches,Firewalls and Proxies

We will expand a bit on SYN cookie is a technique used to resist [SYN flood](https://en.wikipedia.org/wiki/SYN_flood) attacks. The technique's primary inventor [Daniel J. Bernstein](https://en.wikipedia.org/wiki/Daniel_J._Bernstein) defines SYN cookies as "particular choices of initial [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) sequence numbers by TCP servers." In particular, the use of SYN cookies allows a server to avoid dropping connections when the SYN queue fills up. Instead, the server behaves as if the SYN queue had been enlarged. The server sends back the appropriate [SYN+ACK](https://en.wikipedia.org/wiki/SYN%2BACK) response to the client but discards the SYN queue entry. If the server then receives a subsequent ACK response from the client, the server is able to reconstruct the SYN queue entry using information encoded in the TCP sequence number.

**RST ATTACK**

Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

**PING FLOOD – ICMP FLOOD**

Reconfiguring your perimeter firewall to disallow pings will block attacks originating from outside your network, albeit not internal attacks. Still, the blanket blocking of ping requests can have unintended consequences, including the inability to diagnose server issues.

The Incapsula DDoS protection provide blanket protection against ICMP floods by limiting the size of ping requests as well as the rate at which they can be accepted.

**APDoS**

To combat APDoS, organizations require a single vendor, hybrid cyber security solution that protects networks and applications from a wide range of attacks. Ideally, such a solution includes all the different technologies needed for effective detection and mitigation, including DoS/DDoS protection, behavioral analysis, IPS, encrypted attack protection and web application firewall (WAF). Additionally, organizations also require new levels of partnership with their DDoS mitigation service provider and any ISP that provides managed DDoS services to coordinate for the effective detection and mitigation of a multi-vector assault.