National Cybersecurity and Communications Integration Center

29 January 2014

DDoS Quick Guide

Attack Possibilities by OSI Layer

OSI Layer	Protocol Data Unit (PDU)	Layer Description	Protocols	Examples of Denial of Service Techniques at Each Level	Potential Impact of DoS Attack	Mitigation Options for Attack Type
Application Layer (7)	Data	Message and packet creation begins. DB access is on this level. End-user protocols such as FTP, SMTP, Telnet, and RAS work at this layer	Uses the Protocols FTP, HTTP, POP3, & SMTP and its device is the Gateway	PDF GET requests, HTTP GET, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDoS attacks
Presentation Layer (6)	Data	Translates the data format from sender to receiver	Uses the Protocols Compression & Encryption	Malformed SSL Requests -- Inspecting SSL encryption packets is resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server	The affected systems could stop accepting SSL connections or automatically restart	To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host
Session (5)	Data	Governs establishment, termination, and sync of session within the OS over the network (ex: when you log off and on)	Uses the Protocol Logon/Logoff	Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering Telnet services unavailable	Prevents administrator from performing switch management functions	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability
Transport (4)	Segment	Ensures error-free transmission between hosts: manages transmission of messages from layers 1 through 3	Uses the Protocols TCP & UDP	SYN Flood, Smurf Attack	Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Black holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and disrupted service
Network (3)	Packet	Dedicated to routing and switching information to different networks. LANs or internetworks	Uses the Protocols IP, ICMP, ARP, & RIP and uses Routers as its device	ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth	Can affect available network bandwidth and impose extra load on the firewall	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance
Data Link (2)	Frame	Establishes, maintains, and decides how the transfer is accomplished over the physical layer	Uses the Protocols 802.3 & 802.5 and it's devices are NICs, switches bridges & WAPs	MAC flooding -- inundates the network switch with data packets	Disrupts the usual sender to recipient flow of data -- blasting across all ports	Many advances switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered
Physical (1)	Bits	Includes, but not limited to cables, jacks, and hubs	Uses the Protocols 100Base T & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices	Physical destruction, obstruction, manipulation, or malfunction of physical assets	Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets

Possible DDoS Traffic Types

HTTP Header	HTTP headers are fields which describe which resources are requested, such as URL, a form, JPEG, etc. HTTP headers also inform the web server what kind of web browser is being used. Common HTTP headers are GET, POST, ACCEPT, LANGUAGE, and USER AGENT. The requester can insert as many headers as they want and can make them communication specific. DDoS attackers can change these and many other HTTP headers to make it more difficult to identify the attack origin. In addition, HTTP headers can be designed to manipulate caching and proxy services. For example, is it possible to ask a caching proxy to not cache the information.
HTTP POST Flood	An HTTP POST Flood is a type of DDoS attack in which the volume of POST requests overwhelms the server so that the server cannot respond to them all. This can result in exceptionally high utilization of system resources and consequently crash the server.
HTTP POST Request	An HTTP POST Request is a method that submits data in the body of the request to be processes by the server. For example, a POST request takes the information in a form and encodes it, then post the content of the form to the server.
HTTPS Post Flood	An HTTPS POST Flood is an HTTP POST flood sent over an SSL session. Due to the use of SSL it is necessary to decrypt this request in order to inspect it.
HTTPS POST Request	An HTTPS POST Request is an encrypted version of an HTTP POST request. The actual data transferred back and forth is encrypted.
HTTPS GET Flood	An HTTPS GET Flood is an HTTP GET flood sent over an SSL session. Due to the SSL, it is necessary to decrypt the requests in order to mitigate the flood.
HTTPS GET Request	An HTTPS GET Request is an HTTP GET Request sent over an SSL session. Due to the use of SSL, it is necessary to decrypt the requests in order to inspect it.
HTTP GET Flood	An HTTP GET Flood is a layer 7 application layer DDoS attack method in which attackers send a huge flood of requests to the server to overwhelm its resources. As a result, the server cannot respond to legitimate requests from the server.
HTTP GET Request	An HTTP GET Request is a method that makes a request for information for the server. A GET request asks the server to give you something such as an image or script so that it may be rendered by your browsers.
SYN Flood (TCP/SYN)	SYN Flood works by establishing half-open connections to a node. When the target receives a SYN packet to an open port, the target will respond with a SYN-ACK and try to establish a connection. However, during a SYN flood, the three-way handshake never completes because the client never responds to the server's SYN-ACK. As a result, these "connections" remain in the half-open state until they time out.
UDP Flood	UDP floods are used frequently for larger bandwidth DDoS attacks because they are connectionless and it is easy to generate protocol 17 (UDP) messages from many different scripting and compiled languages.
ICMP Flood	Internet Control Message Protocol (ICMP) is primarily used for error messaging and typically does not exchange data between systems. ICMP packets may accompany TCP packets when connecting to a sever. An ICMP flood is a layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth.
MAC Flood	A rare attack, in which the attacker sends multiple dummy Ethernet frames, each with a different MAC address, Network switches treat MAC addresses separately, and hence reserve some resources for each request. When all the memory in a switch is used up, it either shuts down or becomes unresponsive. In a few types of routers, a MAC flood attack may cause these to drop their entire routing table, thus disrupting the whole network under its routing domain.

Glossary

Denial of Service	The core concepts of cyber security are availability, integrity, and confidentiality. Denial of Service (DoS) attacks impact the availability of information resources. The DoS is successful if it renders information resources unavailable. Success and impact differ in that impact is relative to the victim. For example, if an actor DoS's a website belonging to a company that relies on e-commerce to drive their business operations, the company may experience financial losses if the DoS is sustained for a period of time. The risk, threat, and impact levels for DoS activity are determined on a case by case basis.
Layer 3 and Layer 4 DDoS Attacks	Layer 3 and Layer 4 DDoS attacks are types of volumetric DDoS attacks on a network infrastructure Layer 3 (network layer) and 4 (transport layer) DDoS attacks rely on extremely high volumes (floods) of data to slow down web server performance, consume bandwidth, and eventually degrade access for legitimate users. These attack types typically include ICMP, SYN, and UDP floods.
Layer 7 DDoS Attack	A Layer 7 DDoS attack is an attack structured to overload specific elements of an application server infrastructure. Layer 7 attacks are especially complex, stealthy, and difficult to detect because they resemble legitimate website traffic. Even simple Layer 7 attacks--for example those targeting login pages with random user IDs and passwords, or repetitive random searches on dynamic websites--can critically overload CPUs and databases. Also, DDoS attackers can randomize or repeatedly change the signatures of a Layer 7 attack, making it more difficult to detect and mitigate.
itsoknoproblembro	The name given to a suite of malicious PHP scripts discovered on multiple compromised hosts. The main functionalities appear to be file uploads, persistence, and DDoS traffic floods. The itsoknoproblembro toolkit includes multiple infrastructure and application-later attack vectors, such as SYN floods, that can simultaneously attack multiple destination ports and targets, as well as ICMP, UDP, SSL encrypted attack types. A common characteristic of the attacks is a large UDP flood targeting DNS infrastructure. Uniquely, the attacking botnet contains many legitimate (non-spoofed) IP addresses, enabling the attack to bypass most anti-spoofing mechanisms.
PHP Shell, PHP Webshell	A script in the PHP language that can execute commands, view files, and perform other system administrative tasks. PHP shells are often used to take control of web servers via web application vulnerabilities.
Proxy	A proxy is a network device which terminates incoming traffic and then creates a new communication session which is used to send the traffic to the actual destination. The proxy fits between the requestor and the server and mediate all of the communication between the two. Examples of proxy technologies are content switches and load balancers. Proxy servers are most often used for the DNS requests, HTTPS, and HTTP. When HTTPS is being proxied, the proxy server itself must have copies of the public certificate which includes the public key and the private key so it can effectively terminate the SSL/TLS requests. Mitigating Layer 7 DDoS attacks is sometimes carried out using proxies.
Infrastructure DDoS Attack	An infrastructure attack is a DDoS attack that overloads the network infrastructure by consuming large amounts of bandwidth, for example by making excessive connection requests without responding to confirm the connection, as in the case of a SYN flood. A proxy server can protect against these kinds of attacks by using cryptographic hashtags and SYN cookies.
DNS Amplification Attack	A Domain Name Server (DNS) Amplification attack is a popular form of Distributed Denial of Service (DDoS), in which attackers use publically accessible open DNS servers to flood a target system with DNS response traffic. The primary technique consists of an attacker sending a DNS name lookup request to an open DNS server with the source address spoofed to be the target's address. When the DNS server sends the DNS record response, it is sent instead to the target.

Mitigating Large Scale DoS/DDoS Attacks

Device	Layer	Optimized for	DoS Protections
Firewall	4-7	Flow Inspection, Deep Inspection	Screen, Session Limits, Syn Cookie
Router	3-4	Packet Inspection, Frame Inspection	Line-Rate ACLs, Rate Limits

Some DDoS Mitigation Actions and Hardware

- Stateful inspection firewalls
- Stateful SYN Proxy Mechanisms
- Limiting the number of SYNs per second per IP
- Limiting the number of SYNs per second per destination IP
- Set ICMP flood SCREEN settings (thresholds) in the firewall
- Set UDP flood SCREEN settings (thresholds) in the firewall
- Rate limit routers adjacent to the firewall and network

References

http://www.prolexic.com/knowledge-center-dos-and-ddos-glossary.html
http://www.cso.com.au/article/443802/ssl_ddos_attacks_-_growing_trend/
http://jncie.files.wordpress.com/2008/09/801003_protecting-the-network-from-denial-of-service-floods.pdf
http://en.wikipedia.org/wiki/MAC_flooding
http://www.ibrahimhasan.com/content/understanding-and-protecting-against-mac-address-flooding
https://www.owasp.org/images/4/43/Layer_7_DDOS.pdf
http://softwareandnetworks.wordpress.com/
https://www.kb.cert.org/CERT_WEB/services/vul-notes-cert.nsf/b38c0892d481f5d385256d4b005d34ea/e0bf4978a23a358385257179006cb1d8?OpenDocument
http://class10e.com/Microsoft/what-layer-in-the-osi-model-is-responsible-for-logging-on-and-off/
www.books.google.com/books?isbn=1118141350
http://www.wisegeek.com/what-is-mac-flooding.htm
http://quizlet.com/14023507/lesson-2-defining-networks-with-the-osi-model-flash-cards/
http://www.cisco.edu.mn/CCNA_R&S_%28Switched_Networks%29/course/module2/2.2.2.3/2.2.2.3.html
http://www.linuxforu.com/2011/11/cyber-attacks-explained-dos-and-ddos/
http://www.prolexic.com/knowledge-center-dos-and-ddos-glossary.html
http://learnfromtheleader.com/Downloads/SRS/TSFADP.pdf
http://zuhairmirza-informative.blogspot.com/2013/04/dos-and-ddos-glossary-of-terms-part-2.html
http://webcyber.co.uk/?p=128
https://www.cisco.com/web/ME/exposaudi2009/assets/docs/layer2_attacks_and_mitigation_t.pdf
http://www.prolexic.com/knowledge-center-dos-and-ddos-glossary.html
http://www.ddosattacks.biz/ddos-101/glossary/proxy/
http://www.prolexic.com/news-events-pr-end-of-quarter-ddos-attacks-itsok.html
http://www.us-cert.gov/ncas/alerts/TA13-088A