qualitytraining
Succeed with Quality

Networking Training Center of MTI Group

(D)DoS-быстрая справка

18 January 2020

OSI (Open Systems Interconnection) model

	PDU	Layer	Возможные DoS атаки	Потецниальное влияние DoS атак	Возможные меры по защите
L7	Data	Application Network Process to Application	PDF GET requests,HTTP GET, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Нехватка ресурсов сервису, общее ресурсное голодание	Мониторинг приложений (APM), отслеживая zero day и application layer (L7) attack
L6	Data	Presentation Data Representation and Encryption	Посылка неправильных запросов SSL.	Остановка приема SSL соединений, исчерпание ресурсов CPU.	Разгрузка SSL, анализ трафика по признакам использу ADP
L5	Data	Session Internethost Communication	Используются уязвимости сервисов (Longon/Lonoff) К примеру - Telnet	Блокирует администратору доступ к управлению сетевым оборудованием.	Обновлять систему версией устраняющей уязвимость. Ограничивать доступ.
L4	Segments	Transport End-to-End Connections and Reliability	SYN-Flood(TCP/SYN), UDP-Flood, SMURF-attack*	Исчерпание лимитов на подключение, ресурсов CPU, полосы.	Ограничивать кол-во SYN с хоста и общее кол-во, Использовать IDS системы
L3	Packets	Network Path Determination & IP (Logical Addressing)	ICMP-Flood (Ping Flood), Ping of Death (POD), SMURF-attack*	“Забиваются” каналы связи, исчерпание ресурсов CPU	Открывать только нужные типи и коды ICMP, ограничи-вать кол-во ICMP пакетов.
L2	Frames	Data Link MAC and LLC (Physical addressing)	MAC-Flooding, MAC-Spoofing, STP-attack, DHCP-Snooping, ARP-spoofing	Нарушение обычного потока данных SRC-MAC -> DST-MAC	Использовать современные управляемые Switch
L1	Bits	Physical Media, Signal, and Binary Transmission	Физическое уничтожение, повреждение, помехи.	Физические активы будут не функциональны, недоступны	Физическое ограничение доступа к активам. Контрль доступа.

*Smurf attack - многими международными компаниями занимающимися безопасностью классифицируются как атака L4, многими L3