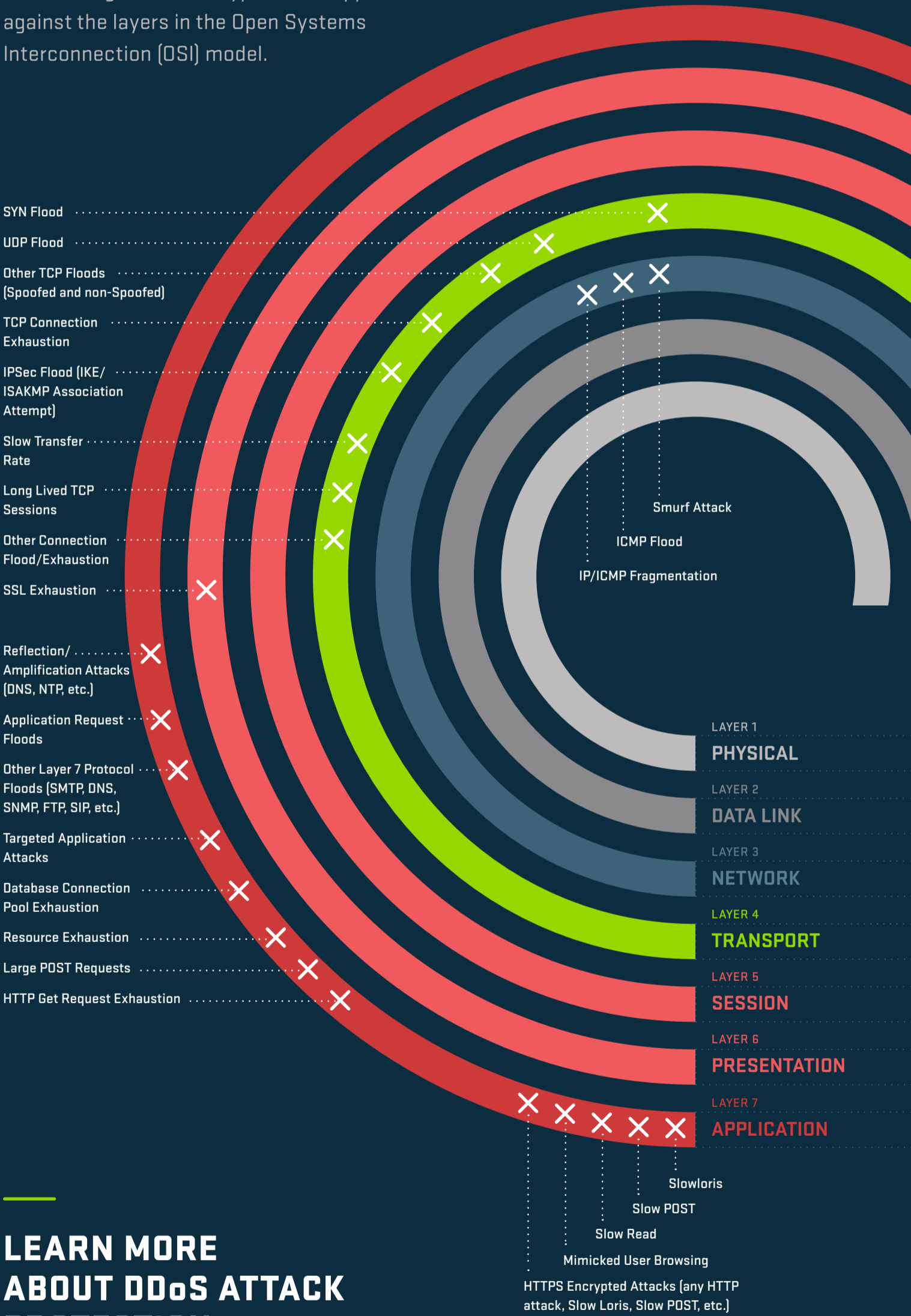# DDoS ATTACK TYPES
ACROSS NETWORK LAYERS OF THE OSI MODEL

A Denial of Service (DoS) attack attempts to deny a user access to a network resource or service. A Distributed Denial of Service (DDoS) attack originates from multiple sources, making it far more difficult to defend.

Here, a range of attack types are mapped against the layers in the Open Systems Interconnection (OSI) model.

SYN Flood

UDP Flood

Other TCP Floods
(Spoofed and non-Spoofed)

TCP Connection
Exhaustion

IPSec Flood (IKE/
ISAKMP Association
Attempt)

Slow Transfer
Rate

Long Lived TCP
Sessions

Other Connection
Flood/Exhaustion

SSL Exhaustion

Reflection/
Amplification Attacks
(DNS, NTP, etc.)

Application Request
Floods

Other Layer 7 Protocol
Floods (SMTP, DNS,
SNMP, FTP, SIP, etc.)

Targeted Application
Attacks

Database Connection
Pool Exhaustion

Resource Exhaustion

Large POST Requests

HTTP Get Request Exhaustion

Smurf Attack

ICMP Flood

IP/ICMP Fragmentation

LAYER 1
PHYSICAL

LAYER 2
DATA LINK

LAYER 3
NETWORK

LAYER 4
TRANSPORT

LAYER 5
SESSION

LAYER 6
PRESENTATION

LAYER 7
APPLICATION

Slowloris

Slow POST

Slow Read

Mimicked User Browsing

HTTPS Encrypted Attacks (any HTTP
attack, Slow Loris, Slow POST, etc.)

LEARN MORE ABOUT DDoS ATTACK PROTECTION

ARBOR NETWORKS®

The Security Division of NETSCOUT