Risico analyse

# Applicatielaag

Applicatie laag DDOS-aanvallen $https://conference.apnic.net/data/37/l7ddos\_apricot\_1393257782.pdf$

$https://www.youtube.com/watch?v=BYKnBki2WTc$

layer 4 ddos = 100 gebruikers leggen 1 site plat (veel gebruikers met 1 doelwit) al de bandbreedte wordt gebruikt. low orbit ion canon,

layer 7 dos = 1 gebruiker legt site plat

vb. R-U-Dead-Yet, niet complete dingen sturen naar IIS, maakt de server unavailble $https://www.youtube.com/watch?v=k1o9Ya8qxlU$ $https://code.google.com/p/r-u-dead-yet/$

XerXes DOs, lokale host maakt aanvalt en is anoniem en geen firewall kan beveiligen $http://www.securitytube.net/video/7530$

SQL Injectie = $https://www.acunetix.com/websitesecurity/sql-injection/$

# Transportlaag

Aanvallen tegen TLS/SSL = voorbeeld $http://en.wikipedia.org/wiki/Transport\_Layer\_Security$

TCP flooding = $http://searchsecurity.techtarget.com/definition/SYN-flooding$ $https://samsclass.info/123/proj10/sockstress.htm$

Sockstress = $https://www.youtube.com/watch?v=hKj\_Dwyt0a0$

port scanning = $http://www.garykessler.net/library/is\_tools\_scan.html$  
🡪 oplossing: http://en.wikipedia.org/wiki/Port\_knocking

# Internetlaag

Oplossing Ping flood = Since ICMP packets should be rare in a normal traffic situation, F5 BIG-IP Local Traffic Manager (LTM) and BIG-IP Advanced Firewall Manager (AFM) are able to mitigate ICMP floods by limiting the rate of all ICMP traffic, and then dropping all ICMP packets above this limit. BIG-IP LTM and BIG-IP AFM provide the ability to set a limit on the maximum number of ICMP packets to prevent the server from ever getting flooded.