Tutorial ICT

Bersama FIRKHAN
firkhan.uthm@yahoo.com

Serangan menerusi protokol HTTP

LALU lintas *Hyper Text Transfer Protocol* (HTTP) menguasai Internet dengan pelayar internet menghubungkan dengan segala-galanya dalam talian. Begitu juga, pusat data mengalami jumlah lalu lintas HTTP yang tinggi termasuk syarikat perniagaan yang melihat lebih banyak hasil daripada jualan dalam talian.

Penggunaan protokol HTTP ini terdedah kepada serangan. Penyerang menggunakan teknik serangan *Denial-of-Service* (DoS) untuk membuat penafian perkhidmatan di pelayan web. Serangan seperti ini digunakan bertujuan untuk membuat keuntungan atau semata-mata hobi. Seterusnya dibincangkan serangan biasa DDoS (*Distributed DoS*) yang dilancarkan terhadap pelayan HTTP.

Pertamanya, HTTP ini berfungsi menerusi capaian protokol TCP (*Transmission Control Protocol*).Oleh itu, pelayan sesawang boleh menghadapi banyak serangan berkaitan dengan protokol TCP seperti serangan SYN *flood*, ACK *floods*, RST *floods*, *Push-ACK floods*, *FIN floods* dan kombinasi antaranya. Lewahan isyarat komunikasi seperti SYN, ACK, RST dan lain-lain dalam rangkaian dimanipulasi sehingga melumpuhkan sistem komunikasi digital.

Keduanya, sambungan protokol HTTP antara penghantar dan penerima data membolehkan beberapa serangan terhadap sambungan tersebut. Antaranya adalah seperti yang berikut.

1 **Serangan *Garbage flood*** - Lewahan data binari kepada pelabuh (*port*) HTTP yang dibuka sehingga melumpuhkan sistem komunikasi digital.

2 **Serangan GET *flood*** - Lewahan isyarat elektronik GET sehingga melumpuhkan sistem komunikasi digital.

3 **Serangan *HEAD* and *POST* *flood*** - Lewahan isyarat elektronik *HEAD* atau *POST* sehingga melumpuhkan sistem komunikasi digital.

4 **Serangan *Reverse Bandwidth floods*** - Lewahan isyarat sambungan internet secara tidak sah sehingga melumpuhkan sistem komunikasi digital.

5 **Serangan HTTP *fuzzers and misbehaved fields*** - Lewahan data atau nilai tidak perlu ke dalam medan dalam protocol HTTP sehingga melumpuhkan sistem komunikasi digital.

6 **Serangan *Cache bypassing*** - Manipulasi maklumat keselamatan kepada pelayan web sehingga mengelirukan fungsi keselamatan pelayan *web* dalam melepaskan serangan yang dibuat.

7 **Serangan *Low and slow*** - Manipulasi maklumat lalu lintas dan insyaratnya menerusi protokol HTTP.

Kebanyakan serangan yang dibuat menggunakan protokol HTTP ini menjurus kepada serangan DoS atau DDoS. Namum begitu, serangan ini boleh dikaitkan kepada perkhidmatan Internet yang lain seperti pelayan DNS, pelayan web dan apa sahaja yang berkait dengannya. Dengan ini, agak kritikal bagi menggantikan penggunaan protokol HTTP ini secara sepenuhnya dengan protokol HTTPS yang lebih selamat.