Γιώργος Σπηλιώτης
IT Consultant

WEB APPLICATION FIREWALLS: ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΕΠΙΘΕΣΕΙΣ ΤΥΠΟΥ SLOWLORIS & R-U-D-Y

Έκτακτη Είδηση! HEARTBleed

- OpenSSL v.1.0.1 έως v.1.0.1f
- Apache & Nginx περίπου 60% των sites
- Ζητάμε echo 64bytes για Block 1 byte
- Λάθος κατά το implementation του echo
- Τι δεδομένα μπορούμε να ανακτήσουμε;
  - Private Keys
  - Unencrypted requests
- Ελέγξτε πρώτα το site με την υπηρεσία της Qualys SSL labs
- Αλλάξτε passwords ΤΩΡΑ!

WAF - Τι είναι;

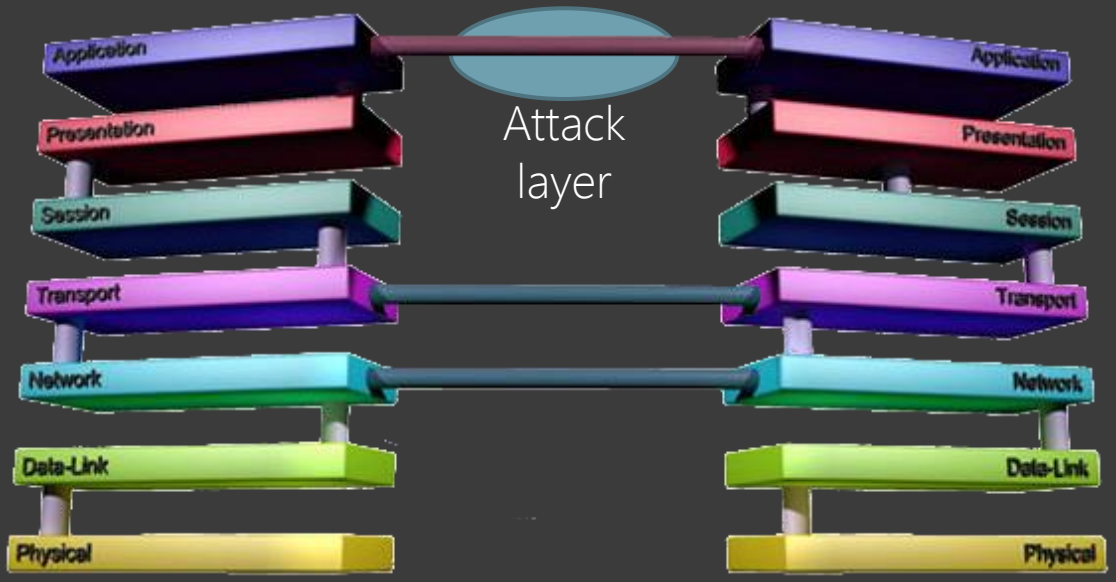
- Firewall σε επίπεδο 7 (layer 7).
- «Καταλαβαίνει» το πρωτόκολλο της εφαρμογής (http).
- Προσπαθεί να εντοπίσει επιθέσεις στο επίπεδο του πρωτοκόλλου HTTP:
  - Λάθη στην εκτέλεση του πρωτοκόλλου (protocol anomalies).
  - Obfuscated arguments: Base64 encoded
  - SQL injections
  - XSS attacks
  - Γνωστά trojan
  - Known Application misconfigurations
  - Μεταβολή εξερχόμενων errors

WAF – Σε ποιους απευθύνεται

- Σε οποιονδήποτε προβάλει ένα internet-facing application:
  - Webmail.
  - Εταιρικές σελίδες.
  - Cloud applications.
  - Forum.
  - Web hosting.
- Σε όσους θέλουν να καταλάβουν/ αναλύσουν ενδεχόμενα attacks:
  - Honeypots.
  - Real-time blocking.
  - Blacklist notifications.

Μα έχω καλό firewall!

- Layer 3 & 4 μόνο.
- IPs & ports.
- Statefull firewall το πολύ μέχρι το επίπεδο transport .



(D)DOS επιπέδου 7

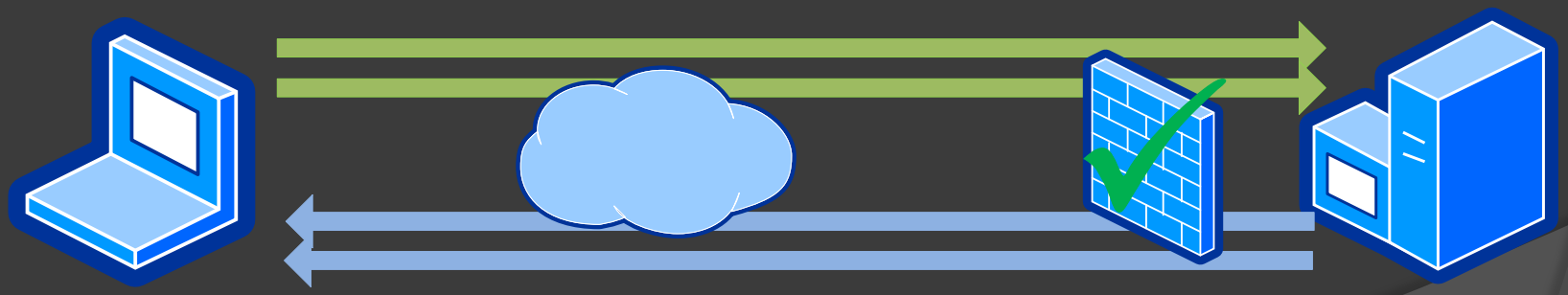
- Σκοπός: να εξαντλήσει τους πόρους εξυπηρέτησης του συστήματος (π.χ. Web Servers)
- Χωρίς την ανάγκη botnet ή amplification attack, λιγότερα connections – low bandwidth/high efficiency
- Δύσκολο να εντοπιστεί η επίθεση (φυσιολογικά connections) – higher obscurity

Με εμένα θα ασχοληθούν;

- Αύξηση κατά 43% ετησίως των Layer 7 επιθέσεων.
- Πολύ εξειδικευμένες επιθέσεις.
- Προσπερνούν εύκολα τα firewall/IDS.
- Με χαμηλά resources πετυχαίνουν το μέγιστο αποτέλεσμα.
- Δύσκολος ο εντοπισμός άρα μπορούν να είναι ενεργές για πολλές ώρες/μέρες.

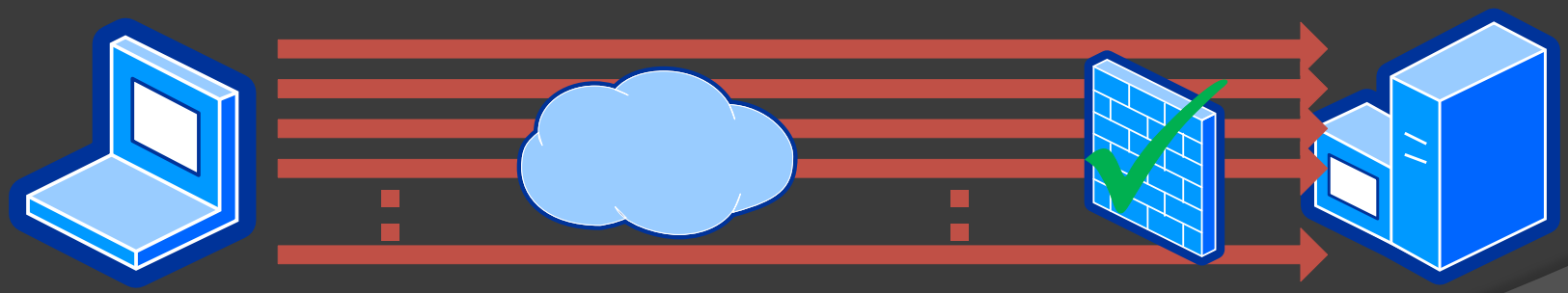
Slowloris: Normal request

GET /docs/walkme/settings.txt?callback=fixedCallback&_=1393170097705 HTTP/1.1
Host: www.example.com
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.117 Safari/537.36
Referer: https://www.example.com/frameset.phtml?.sess=oOyTr87HHCWHoMVMKNj4-McHJYY.
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: timestamp=oeu98[illegible]0008804r0.21094444304705; __id=VYFJZPZMU5H7TK4KRWGUAL%3A2013



Slowloris: Slow request

GET /docs/walkme/settings.txt?callback=fixedCallback&_=1393170097705 HTTP/1.1
Host: www.example.com
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.117 Safari/537.36
Referer: https://www.example.com/frameset.phtml?.sess=oOyTr87HHCWHoMVMKNj4-McHJYY.
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: timestamp=oeu98[illegible]0008804r0.21094444304705; __id=VYFJZPZMU5H7TK4KRWGUAL%3A2013
SlowHeader: 123...



Slowloris: mitigation

- HTTP timeout: header completion (IIS)
- Περιορισμός των ταυτόχρονων συνδέσεων ανά IP
- Περιορισμός των διαδοχικών requests ανά IP
- mod_security directive (>= v2.5.13)

```
SecReadStateLimit 5
```

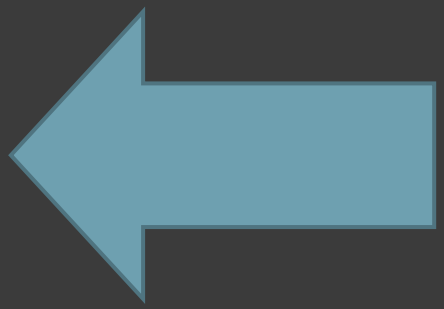
HTTP POST DDOS attack

- Εκμεταλλευόμαστε ότι το POST request έχει Content-Length (δηλαδή «σώμα»).
- POST request πριν το authentication:
  - Login prompt.
  - Registration form (forum).
  - Δημοσκοπήσεις (poll).
  - Page/Site settings.

Slow POST: Πως γίνεται

POST /cgi/login.cgi HTTP/1.1
Host: www.example.com
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.117 Safari/537.36
Content-Length: 10000

&System_ID=123456….
&Account_ID=1234567….
&password=123456789…..
.
.



HTTP POST DDOS attack

- Αν κάνουμε enforce timeout με βάση το content-length πόσο θα ήταν αυτό;
- Οι mobile users δεν έχουν πάντα μεγάλο bandwidth.
- HTTP/1.1 & chunked-encoding = άγνωστο Content Length.
- Περιορισμοί με βάση το IP;
- Ανάλυση κάθε δυνατού POST της εφαρμογής και του μέγιστου χρόνου (speed floor);

HTTP POST DDOS attack

- Ονομάζεται και RUDY attack (από το όνομα του script: R-U-Dead-Yet)
- Έτοιμο script https://code.google.com/p/slowhttptest/
- IIS 7 >20.000 connections ανεξάρτητα από το hardware [rapid fail protection sandbox]
- Apache >10.000 connections [default config]

Slow HTTP POST: mitigation

- Mod_security: **SecWriteStateLimit**
- Apache + mod_security:
  - mod_reqtimeout:
    RequestReadTimeout header=30, body=30
  - mod_security:

```
SecRule RESPONSE_STATUS "@streq 408" \
"phase:5,t:none,nolog,pass, \
setvar:ip.slow_dos_counter=+1,expirevar:ip.slow_dos_cou
nter=60"
SecRule IP:SLOW_DOS_COUNTER "@gt 5" \
"phase:1,t:none,log,drop, \
msg:'Client Connection Dropped due to high # of slow
DoS alerts'"
```

Συμπεράσματα

- Χρήση Web Application Firewall.
- Καλή γνώση του WAF & fast response.
- Μεγάλη ορατότητα της δικτυακής κίνησης και εργαλεία ανάλυσης.
- Όχι σε plug, play & forget λύσεις της αγοράς.
- Χρήση CDN όπου είναι δυνατόν.
- DNS switching με ελάχιστο χρόνο propagation (< 5mins).
- DarkIPs για διαχωρισμό των IP της φυσιολογικής κίνησης.