Hihat

**Τι είναι το Hihat**

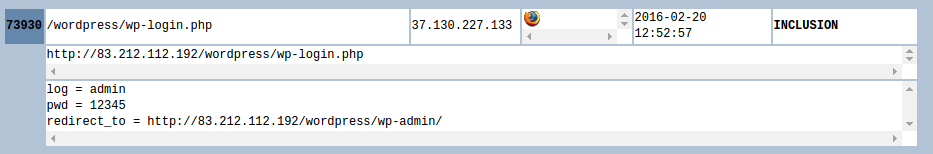
Το Hihat (High Interaction Honeypot Analysis Toolkit) έχει τη δυνατότητα να μετατρέπει εφαρμογές βασισμένες σε PHP κώδικα σε υψηλής αλληλεπίδρασης διαδικτυακά honeypot. Ακόμη, παρέχει γραφικό περιβάλλον διεπαφής χρήστη για την παρακολούθηση του honeypot και για την ανάλυση των αποτελεσμάτων.

Μερικά παραδείγματα εφαρμογών που μπορούν να μετατραπούν σε διαδικτυακά honeypot είναι το WordPress, το PHPMyAdmin και το PHPNuke.

**Βασικές δυνατότητες του Hihat**

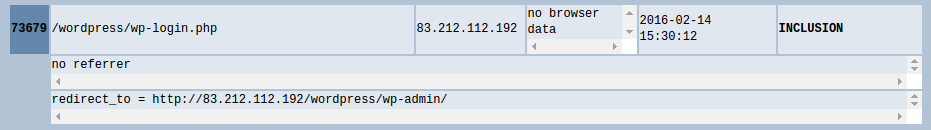
1. Παρουσίαση των συμβάντων για κάθε ιστότοπο σε μία συνολική οθόνη
2. Δυνατότητα έρευνας για επιθέσεις που έχουν πραγματοποιηθεί, με βάση το ID μίας επίθεσης, σύμφωνα με ένα σύνολο IDs ή με βάση ένα συγκεκριμένο τύπο επίθεσης όπως SQL
3. Έλεγχος για ποια αρχεία έχουν ληφθεί από τους διαφορετικούς ιστότοπους σε μία ενιαία οθόνη
4. Παρουσίαση στατιστικών αποτελεσμάτων καθώς και γεωεντοπισμός των επιθέσεων με χρήση google maps

**Τύποι επιθέσεων που υποστηρίζονται**

1. **Inclusion**: Αφορά την προσπάθεια του επιτιθέμενου να αποκτήσει πρόσβαση στο σύστημα, δίνοντας ένα username και ένα password. Είναι δυνατό να συνδυαστεί με επιθέσεις τύπου SQL

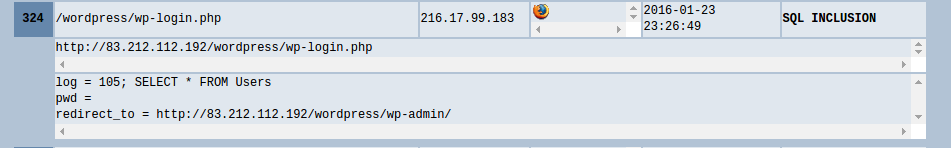
*Εικόνα: Παράδειγμα επίθεσης τύπου Inclusion (πηγή: Hihat)*

Ακόμη, μία προσπάθεια απόκτησης ενός αρχείου με εντολές **WGET** και **CURL** χαρακτηρίζεται από το Hihat ως **Inclusion** στη σελίδα που πραγματοποιήθηκε η εντολή όπως



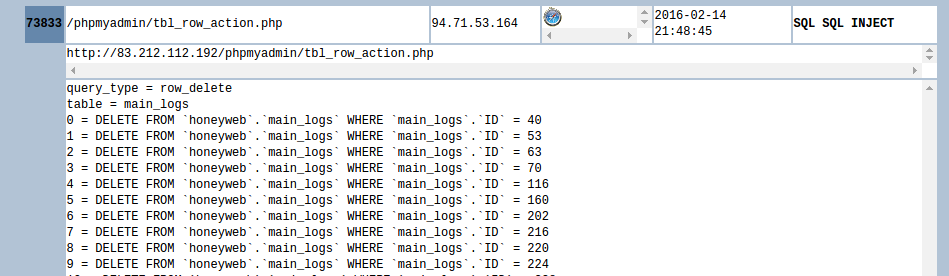
*Εικόνα: Παράδειγμα απόκτησης αρχείου με χρήση εντολών WGET και CURL(πηγή: Hihat)*

1. **SQL**: Αφορά εντολές που δίνονται από τον επιτιθέμενο σε σημεία όπου είναι δυνατό να προστεθεί κείμενο, όπως σε HTML input forms. Χωρίζονται σε SQL Inclusion και SQL Injection.
   1. **SQL Inclusion**: Καταγράφεται από το σύστημα ως επίθεση αυτού του τύπου όταν ο επιτιθέμενος τοποθετήσει την εντολή σε input form όπου πραγματοποιείται ταυτοποίηση του χρήστη, όπως στο wplogin.php του WordPress



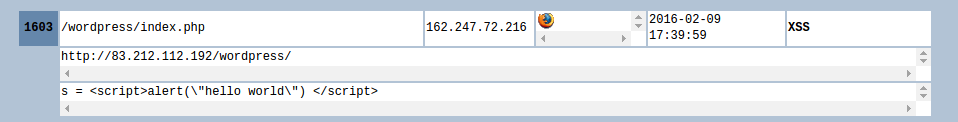
*Εικόνα: Παράδειγμα επίθεσης τύπου SQL Inclusion (πηγή: Hihat)*

* 1. **SQL Injection**: Καταγράφεται ως επίθεση αυτής της μορφής όταν ο επιτιθέμενος τρέξει μία SQL εντολή και επιτύχει να επηρεάσει τη βάση του αντίστοιχου site, όπως μέσω του PHPMyAdmin



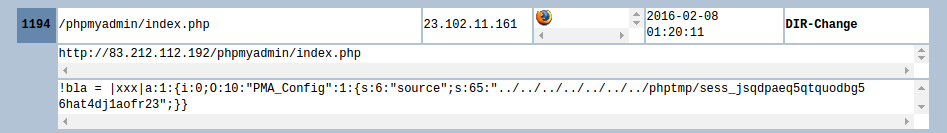
*Εικόνα: Παράδειγμα επίθεσης τύπου SQL Injection (πηγή: Hihat)*

1. **XSS**: Το σύστημα καταγράφει μία επίθεση ως αυτού του τύπου όταν ο επιτιθέμενος προσθέσει σε ένα input form οποιουδήποτε τύπου ένα ‘’client side script ‘’ όπως JavaScript.



*Εικόνα: Παράδειγμα επίθεσης τύπου XSS (πηγή: Hihat)*

1. **DIR – Change**: Η επίθεση αυτής της μορφής δίνει τη δυνατότητα στον επιτιθέμενο, όταν είναι επιτυχής, να πάρει πρόσβαση σε αρχεία του συστήματος που δε θα έπρεπε να έχει πρόσβαση μέσω του web server, όπως το /etc/shadow



*Εικόνα: Παράδειγμα επίθεσης τύπου DIR-Change (πηγή: Hihat)*

1. **Deface:** Επιθέσεις αυτής της μορφής αφορούν την αλλαγή του index.php και άλλων σελίδων, με σελίδες επιλεγμένες από τον επιτιθέμενο. Είναι γνωστές και ως επιθέσεις ‘’electronic graffiti’’. Στις ιστοσελίδες μας δεν παρατηρήθηκε επίθεση αυτής της μορφής

**Υλοποίηση του Hihat**

Η υλοποίηση του παραπάνω εργαλείου πραγματοποιήθηκε σε VPS στην πλατφόρμα Okeanos με τα παρακάτω στοιχεία:

|  |  |
| --- | --- |
| Διεύθυνση IPv4 | 83.212.112.192 |
| Λειτουργικό σύστημα | Ubuntu 12.04.5 LTS |
| Διαθέσιμοι επεξεργαστές (CPU) | 1 |
| Διαθέσιμος χώρος δίσκου | 40 GB |
| Διαθέσιμη προσωρινή μνήμη (RAM) | 4 GB |

*Πίνακας : Χαρακτηριστικά του snf-694389 VPS που χρησιμοποιήθηκε για την υλοποίηση του Hihat honeypot.*

Σε αυτό το σημείο αξίζει να αναφερθεί ότι η έκδοση αυτή των *Linux Ubuntu 12.04.5* δεν επιλέχθηκε τυχαία. Το εργαλείο, χρησιμοποιεί μία παλαιότερη έκδοση της PHP, η οποία δεν είναι συμβατή με εκδόσεις μεγαλύτερες της 5.4. Συνεπώς για να γίνει η εγκατάσταση αυτής της έκδοσης με τον απλούστερο και περισσότερο σταθερό τρόπο, επιλέχθηκε η εγκατάσταση της παραπάνω έκδοσης των Linux.

**Εργαλεία που χρησιμοποιήθηκαν**

Apache server, MySQL database, PHP στην οποία είναι βασισμένη η υλοποίηση των ιστότοπων του WordPress, PHPMyAdmin όπως και του εργαλείου Hihat.

**Εγκατάσταση**

Αρχικά απαιτείται η εγκατάσταση του πακέτου LAMP (Linux, Apache, MYSQL, PHP). Σύμφωνα με τις πληροφορίες από τον [ιστότοπο](https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-ubuntu):

1. **Εγκατάσταση του server Apache:** Απαιτείται η εκτέλεση των παρακάτω 2 εντολών
   1. sudo apt-get update
   2. sudo apt-get install apache2
2. **Εγκατάσταση της MYSQL ως βάση δεδομένων:** Απαιτείται η εκτέλεση των εντολών
   1. sudo apt-get install mysql-server libapache2-mod-auth-mysql php5-mysql
   2. sudo mysql\_install\_db
   3. sudo /usr/bin/mysql\_secure\_installation (Σε αυτό το κομμάτι αρκεί η τοποθέτηση μονάχα του root password, ώστε το honeypot που θα δημιουργηθεί να έχει ένα επίπεδο πολυπλοκότητας για τον επιτιθέμενο, όμως να είναι τελικώς προσβάσιμο και ‘’ανοικτό’’ σε επιθέσεις)
3. **Εγκατάσταση της PHP:** Είναι απαραίτητη η εκτέλεση των εντολών
   1. sudo apt-get install php5 libapache2-mod-php5 php5-mcrypt

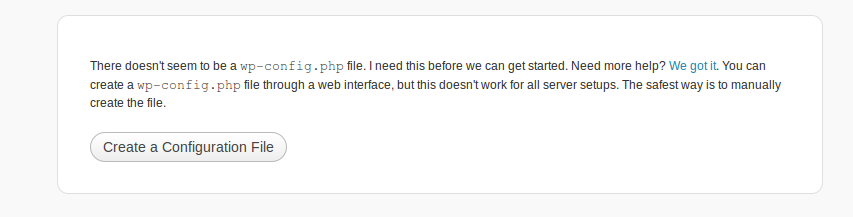
Οι υπόλοιπες εντολές που αναφέρονται στο *tutorial* δεν είναι απαραίτητες για την εγκατάσταση του εργαλείου

1. **Επιβεβαίωση εγκατάστασης της PHP**: Εκτέλεση των εντολών
   1. sudo nano /var/www/info.php
   2. *<?php phpinfo(); ?>* (Τοποθέτηση του κώδικα αυτού μέσα στο αρχείο *info.php*)
   3. sudo service apache2 restart
   4. Άνοιγμα ενός φυλλομετρητή στη σελίδα που βρίσκεται ο server/info.php

(Παράδειγμα: http://12.34.56.789/info.php)

Στη συνέχεια πρέπει να γίνει η εγκατάσταση του **WordPress** και του **PHPMyAdmin**

1. **Εγκατάσταση WordPress:** Από την παρακάτω [ιστοσελίδα](https://wordpress.org/download/release-archive/) κατεβάζουμε την έκδοση του WordPress που μας ενδιαφέρει. Για την εγκατάστασή μας προτείνεται η έκδοση 3.0.4 η οποία μπορεί να ληφθεί από [εδώ](https://wordpress.org/wordpress-3.0.4.zip)
   1. Αφού ολοκληρωθεί η λήψη το κάνουμε extract στο */var/www/* στο Ubuntu 12.04 μηχάνημα και πηγαίνουμε *στην IP του μηχανήματος/WordPress* (με την προϋπόθεση ότι έτσι ονομάζεται ο φάκελος που περιέχει τα αρχεία). Εμφανίζεται η παρακάτω οθόνη:

****

*Εικόνα: Στιγμιότυπο από την εγκατάσταση του WordPress τη στιγμή κατά την οποία ζητείται το configuration file (πηγή: WordPress)*

* 1. Πατώντας το ‘’Create a configuration file’’ προκύπτει η παρακάτω οθόνη στην οποία τοποθετούμε τα απαραίτητα στοιχεία ολοκληρώνοντας την εγκατάσταση του WordPress



*Εικόνα: Στιγμιότυπο από την εγκατάσταση του WordPress τη στιγμή κατά την οποία ζητούνται τα στοιχεία του χρήστη στο σύστημά του (πηγή: WordPress)*

1. **Εγκατάσταση του PHPMyAdmin:** Η εγκατάσταση στηρίζεται στο tutorial της παρακάτω [ιστοσελίδας](https://www.digitalocean.com/community/tutorials/how-to-install-and-secure-phpmyadmin-on-ubuntu-12-04)
   1. Εκτελούμε την εντολή: *sudo apt-get install phpmyadmin apache2-utils*
   2. Στη συνέχεια εκτελούμε την *sudo nano /etc/apache2/apache2.conf* και προσθέτουμε σε όποιο σημείο του αρχείου την

*Include /etc/phpmyadmin/apache.conf*

* 1. Τέλος κάνουμε restart τον apache server: *sudo service apache2 restart*
  2. Δεν απαιτείται το τελευταίο μέρος σχετικά με το *Security* που αναφέρεται στο tutorial καθώς επιθυμούμε ο επιτιθέμενος να έχει τη δυνατότητα να χτυπήσει την ιστοσελίδα

1. **Εγκατάσταση του εργαλείου Hihat:** Η εγκατάσταση στηρίζεται στο tutorial που παρέχεται από το δημιουργό του εργαλείου το οποίο βρίσκεται [εδώ](http://hihat.sourceforge.net/installation.html), συν κάποιες επιπλέον πληροφορίες από την εμπειρία μας κατά την εγκατάστασή του στο δικό μας μηχάνημα

**Προετοιμασία του log server**

* 1. Δημιουργία μίας βάσης δεδομένων με όνομα ‘*’honeyweb’’*
  2. Import του αρχείου ‘*’HIHAT-Create-Tables.sql’’* το οποίο όμως απαιτείται να έχει την παρακάτω [μορφή](HIHAT-Create-Tables.sql) για λόγους συμβατότητας με τη MYSQL βάση που εισαγάγαμε παραπάνω
  3. Δημιουργία ενός login profile, πχ με όνομα *honeyuser*, και περιορισμός των δικαιωμάτων πρόσβασής του μόνο στη βάση *honeyweb* για λόγους ασφαλείας
     1. Σε αυτό το σημείο αξίζει να αναφερθεί ότι προσπαθήσαμε να τοποθετήσουμε τη βάση σε ξεχωριστό Vm, στο δικό μας υπολογιστή, που όμως λόγω της χαμηλής ταχύτητας σύνδεσης στο διαδίκτυο (στη δική μας περίπτωση 4 Mbps downlink, 1Mbps Uplink) οδηγούσε σε πολύ υψηλό χρόνο φόρτωσης και του Hihat web interface αλλά και των άλλων 2 ιστοσελίδων που έτρεχαν στον Okeano. Αποτέλεσμα των παραπάνω ήταν η απόφαση για τοποθέτηση της βάσης στο ίδιο μηχάνημα, του Okeanos.

**Εγκατάσταση του διαδικτυακού Honeypot**

* 1. Επιλογή ποιου από τα δύο, στην περίπτωσή μας, *WordPress*, *PHPMyAdmin*, θα μετατρέψουμε σε Honeypot πρώτο. Η διαδικασία θα επαναληφθεί αντίστοιχα για τον άλλο ιστότοπο με τον ίδιο τρόπο στη συνέχεια
  2. Μετονομασία του αρχείου *insertionFile.txt* σε *Insertionfile.txt.*
  3. Άνοιγμα του αρχείου *Insertionfile.txt* και μετονομασία της μεταβλητής *$thisModule\_23cdx\_* στο όνομα που επιλέγουμε να έχει το Honeypot μας.

Πχ στο WordPress Honeypot μας μπορούμε να την ονομάσουμε

*$thisModule\_23cdx\_ = "WordPress";*

* 1. Στο ίδιο αρχείο η *γραμμή 27* πρέπει να γίνει

*$link23 = mysql\_connect("localhost", "honeyuser", "honeypass", true );*

όπου το *localhost* παραμένει το ίδιο, *honeyuser* είναι το όνομα του χρήστη που δημιουργήσαμε για να χειρίζεται τη βάση του Hihat και περιορίσαμε τα προνόμια του μόνο για αυτή τη βάση, *honeypass* είναι το password του παραπάνω χρήστη και το *true* αναφέρεται στο γεγονός ότι ο συγκεκριμένος χρήστης χρησιμοποιεί password.

* 1. Στη συνέχεια απαιτείται η εγκατάσταση ενός Java Environment. Προτείνεται η εγκατάσταση του *OpenJDK*, ο οδηγός για την εγκατάσταση του οποίου μπορεί να βρεθεί [εδώ](https://www.digitalocean.com/community/tutorials/how-to-install-java-on-ubuntu-with-apt-get).
     1. Εκτέλεση της εντολής *sudo apt-get update,* ώστε να γίνουν όλες οι αναβαθμίσεις του ήδη εγκατεστημένου λογισμικού στην τελευταία έκδοση
     2. Εκτέλεση της *java –version*. Αν η απάντηση είναι της μορφής, *The program java can be found in the following packages*, σημαίνει ότι η Java δεν είναι εγκατεστημένη και μπορεί να εγκατασταθεί με την εντολή *sudo apt-get install openjdk-7-jre*.
  2. Εκτέλεση των εντολών
     1. *cd directory where Hihat resides/Honeypot-Creator/*
     2. *java honeypot\_creator /var/www/όνομα directory όπου βρίσκεται το WordPress ή το PHPMyAdmin αντίστοιχα*

**Εγκατάσταση διαδικτυακής διεπαφής του εργαλείου Hihat**

* 1. Δημιουργία ενός νέου φακέλου στην τοποθεσία /var/www/ για την τοποθέτηση της διαδικτυακής διεπαφής του παραπάνω εργαλείου, έστω *Hihat* το όνομά του
  2. Δημιουργία ενός αρχείου .htaccess ή με χρήση του αρχείου httpd.conf για προστασία του φακέλου Hihat
     1. *Προστασία του φακέλου με χρήση του αρχείου .htaccess*
        1. Δημιουργία του αρχείου .htaccess μέσα στο φάκελο Hihat με την εντολή *sudo nano .htaccess.* Το αρχείο πρέπει να έχει την παρακάτω [μορφή](htaccess.txt)
        2. Δημιουργία του αρχείου *.htpasswd* σε ένα directory όπου δε θα έχει πρόσβαση ο web server. Στην περίπτωσή μας όπως φαίνεται από την 3η γραμμή του αρχείου επιλέχθηκε η τοποθεσία */etc/apache2/*

Το .htpasswd αρχείο, εκτός από τον χειροκίνητο τρόπο όπως δημιουργήθηκε και το .htaccess, μπορεί να δημιουργηθεί με την παρακάτω εντολή:

*sudo htpasswd -c /etc/apache2/.htpasswd username*

όπου αναφέρεται η τοποθεσία του αρχείου αμέσως μετά το –c και στο τέλος όπου username είναι το όνομα του χρήστη που θα ζητείται για την πρόσβαση στο φάκελο από το φυλλομετρητή. Μετά την εκτέλεση της εντολής απαιτείται η τοποθέτηση ενός password. Το αρχείο .htpasswd θα έχει τελικώς την παρακάτω [μορφή](htpasswd.txt).

* + 1. *Προστασία του φακέλου με χρήση του αρχείου .httpd.conf*
       1. Εύρεση του παραπάνω αρχείου στην τοποθεσία /etc/apache2
       2. Μετατροπή του αρχείου στην παρακάτω [μορφή](httpd.conf), όπου στη θέση του */var/www/Hihat* πρέπει να τοποθετηθεί η τοποθεσία του φακέλου που θέλουμε να προστατεύσουμε. Επίσης στη γραμμή

*AuthUserFile /etc/apache2/.htpasswd* πρέπει να τοποθετηθεί η τοποθεσία του αρχείου .htpasswd που αναλύσαμε παραπάνω. Η διαδικασία κατασκευής του τελευταίου αρχείου παραμένει η ίδια

* 1. Αντιγραφή των περιεχομένων του φακέλου *HIHAT - Analysis Tool*  στην τοποθεσία /var/www/Hihat όπου Hihat ο προστατευόμενος φάκελος που δημιουργήσαμε πριν
  2. Μετατροπή του αρχείου *inc/constant.php* στην παρακάτω [μορφή](constant.php), όπου *MYSQL\_HOST* είναι το όνομα του host που έχει τη βάση δεδομένων, στην περίπτωσή μας *localhost. MYSQL\_USER* είναι το όνομα του χρήστη της βάσης δεδομένων *honeyweb, MYSQL\_PASS*  το password του παραπάνω χρήστη. Το *GOOGLE\_MAPS\_KEY* μπορεί να μείνει ως έχει καθότι δε χρησιμοποιείται για τον γεωεντοπισμό των επιτιθέμενων.
  3. Με σκοπό την αυτόματη λήψη από το εργαλείο των αρχείων που κατέβασε ο επιτιθέμενος με χρήση *WGET* και *CURL* προτείνεται από τον ιστότοπο του tutorial η χρήση της εντολής *lynx*. Εμείς αντίστοιχα παρατηρήσαμε ότι μία τέτοια στρατηγική έβαζε μεγάλο φόρτο στον server και για αυτό μπαίναμε μέσω ενός φυλλομετρητή (στη δική μας περίπτωση Firefox, παρόλα αυτά είναι εφικτό να γίνει και με άλλους), στη διεύθυνση:

[*http://localhost/your-directory/autodownloader/check\_downloads.php?verobse=false*](http://localhost/your-directory/autodownloader/check_downloads.php?verobse=false)

μία φορά την ημέρα, συνεπώς δεν απαιτούνταν αυτόματο εργαλείο για αυτό το σκοπό.

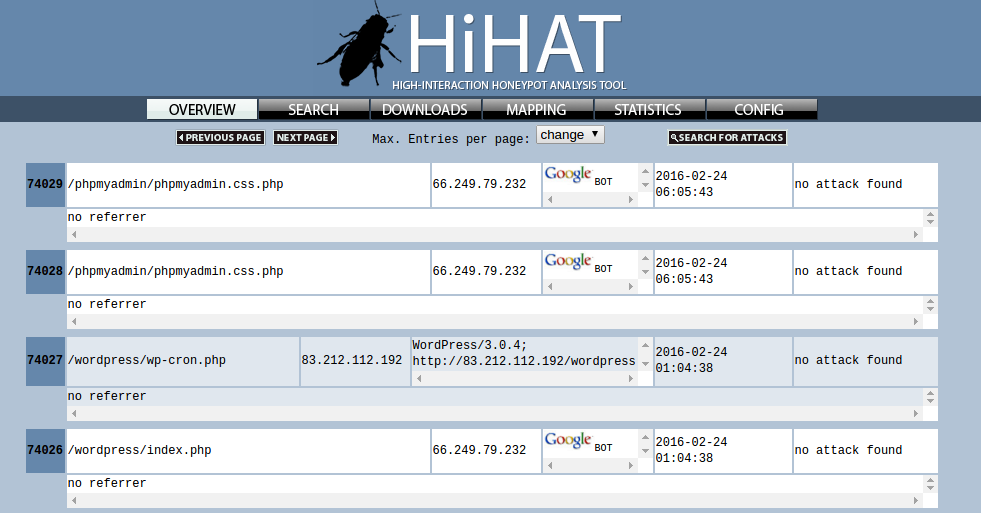
* 1. Για την ενεργοποίηση του γεωεντοπισμού απαιτείται η αλλαγή κάποιων μερών του αρχείου *printMap.php*. Για μεγαλύτερη ευκολία μπορεί απλά να αντικατασταθεί το παραπάνω αρχείο με το <printMap.php> που έχει ήδη αλλαχθεί από εμάς. Η αλλαγή που πραγματοποιήθηκε στο αρχείο αφορούσε την αφαίρεση του *Google Maps Key* καθότι δεν είναι απαραίτητο για τη λειτουργική χρήση του *Mapping* του εργαλείου και προσθέτει σημαντικά μεγαλύτερη πολυπλοκότητα στην παραμετροποίηση.
  2. Τέλος, απαιτείται η λήψη της βάσης δεδομένων που συσχετίζει τις IP με τις θέσεις στο χάρτη. Ο ιστότοπος που επιλέχθηκε ενδεικτικά από εμάς είναι ο [παρακάτω](http://lite.ip2location.com/). Επιλέχθηκε η *DB5.LITE* καθότι δεν απαιτούνταν περισσότερα στοιχεία από την εφαρμογή. Για μεγαλύτερη ευκολία, η βάση με τη μορφή που ελήφθη από εμάς μπορεί να βρεθεί [εδώ](IP2LOCATION-LITE-DB5.CSV.ZIP)

**Παρουσίαση Αποτελεσμάτων**

Ανάμεσα στις ημερομηνίες *10 Ιανουαρίου 2016* με *11 Φεβρουαρίου 2016* προέκυψαν τα παρακάτω:

Αρχική Οθόνη – Overview

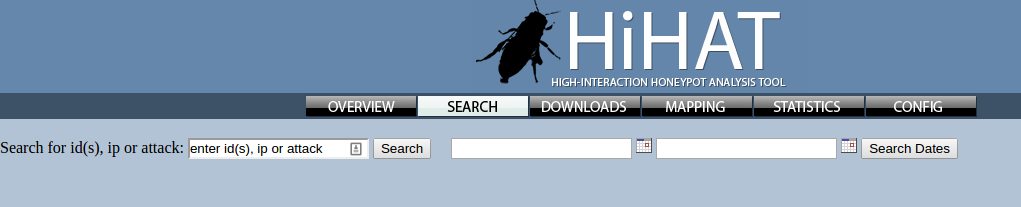
Στην παρακάτω εικόνα βλέπουμε στο πιο αριστερό μέρος το ID της κάθε καταγραφής, δεξιότερα παρατηρούμε τον ιστότοπο που πραγματοποιήθηκε η καταγραφή. Στη συνέχεια, φαίνεται η IP από την οποία εισήλθε ο επιτιθέμενος και ο browser που χρησιμοποίησε, στη δεδομένη περίπτωση Firefox και τέλος εμφανίζεται η ημερομηνία καταγραφής καθώς και αν παρατηρήθηκε κάποιο είδος επίθεσης.



*Εικόνα: Καρτέλα ‘’Overview’ του εργαλείου όπου φαίνονται γενικές πληροφορίες (πηγή: Hihat)*

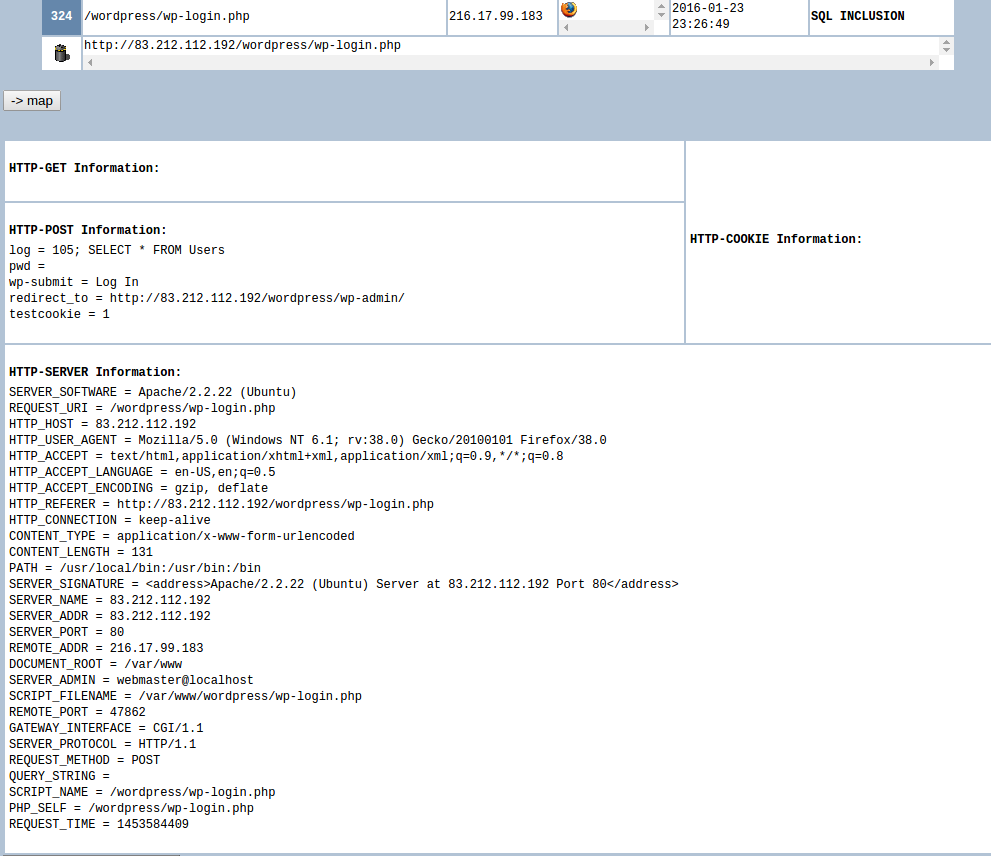
Έρευνα – Search

Σε αυτό το παράθυρο μπορούμε να κάνουμε έρευνα στη βάση δεδομένων με βάση συγκεκριμένα στοιχεία όπως ID, σειρά από IDs, τύπο επίθεσης όπως SQL, καθώς φαίνεται παρακάτω:



*Εικόνα: Καρτέλα ‘’Search’’ του εργαλείου όπου είναι δυνατή η αναζήτηση επιθέσεων (πηγή: Hihat)*

Στη συνέχεια βλέπουμε μία συγκεκριμένη επίθεση καθώς και τις πληροφορίες που εμφάνισε το εργαλείο για αυτή:

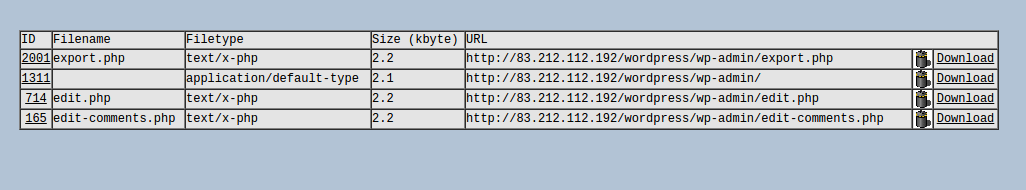


*Εικόνα: Πληροφορίες σχετικά με μία συγκεκριμένη επίθεση (πηγή: Hihat)*

Μπορούμε να παρατηρήσουμε ότι είναι μία επίθεση τύπου *SQL INCLUSION*, ότι η εντολή που χρησιμοποιήθηκε είναι η *SELECT \* FROM USERS,* καθώς και μία πληθώρα πληροφοριών στη συνέχεια όπως η IP του server μας, η έκδοση του apache που χρησιμοποιήσαμε, το πρωτόκολλο του server κ.α.

Στοιχεία που έχουν ληφθεί – Downloads

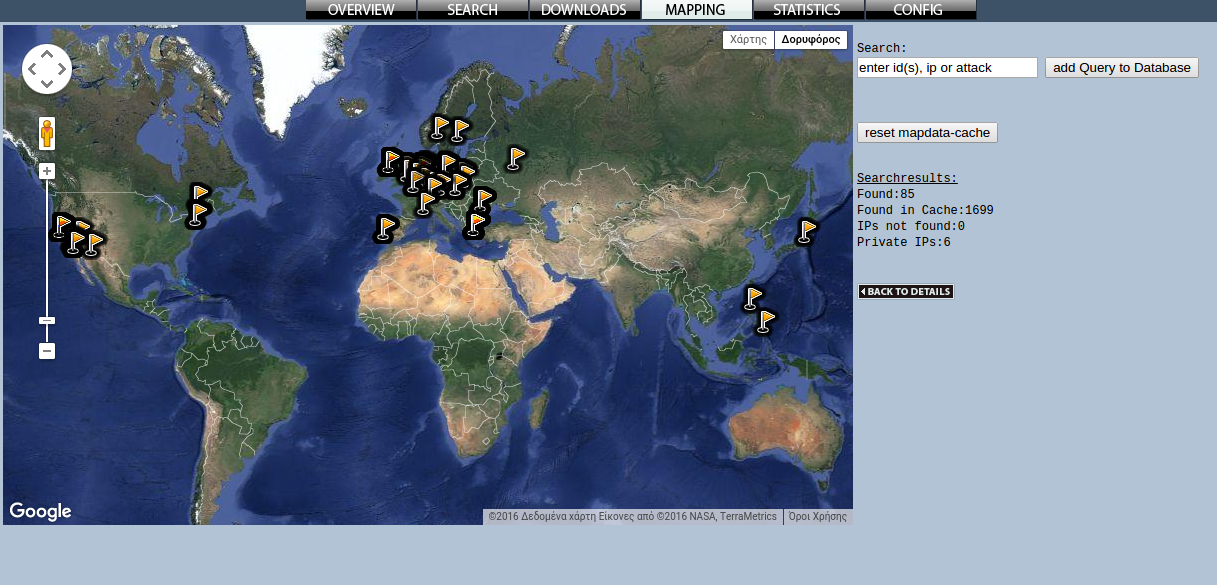
Σε αυτή την καρτέλα μπορούμε να δούμε κάποια τα στοιχεία που έχουν ληφθεί και για κάθε ένα από αυτά πατώντας στην αριστερή πλευρά στο ID, έχουμε τη δυνατότητα να εμφανίσουμε ένα παράθυρο όπως το παραπάνω, με περισσότερες πληροφορίες σχετικά με την επίθεση



*Εικόνα: Καρτέλα ‘’Downloads’’ του εργαλείου όπου εμφανίζονται πληροφορίες σχετικά με κάποια από τα αρχεία που κατέβηκαν από τους επιτιθέμενους (πηγή: Hihat)*

Γεωεντοπισμός επιθέσεων – Geolocation

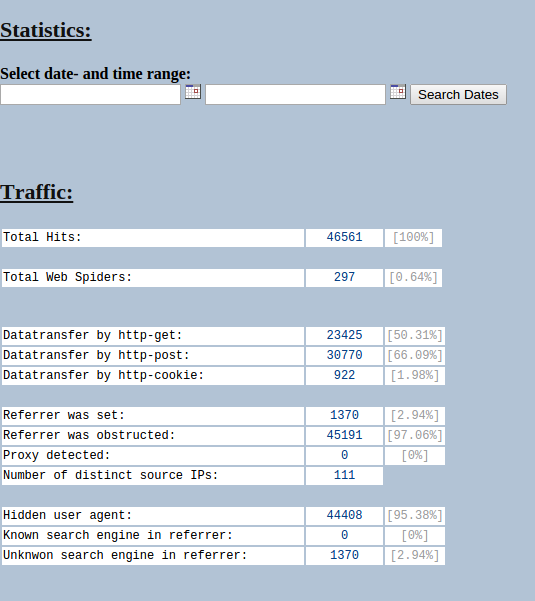
Σε αυτό το σημείο παρατηρούμε τη δυνατότητα γεωεντοπισμού του εργαλείου με βάση συγκεκριμένη έρευνα στηριζόμενη σε κριτήρια ανάλογα της *έρευνας – search* που αναλύσαμε παραπάνω:



*Εικόνα: Καρτέλα ‘’Mapping’’ του εργαλείου όπου γίνεται ο γεωεντοπισμός των επιθέσεων (πηγή: Hihat)*

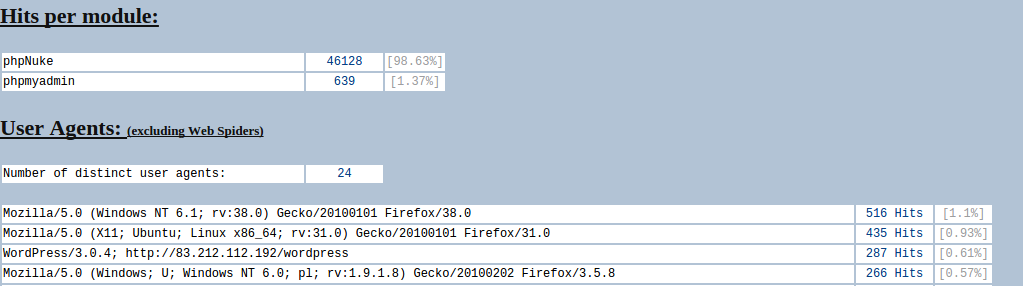
Στατιστικά – Statistics

Αυτή η καρτέλα προσφέρει αναλυτικότερες πληροφορίες σχετικά με το σύνολο των επιθέσεων:



*Εικόνα: Καρτέλα ‘’Statistics’’ του εργαλείου όπου εμφανίζονται πληροφορίες σχετικά με την Κίνηση (πηγή: Hihat)*

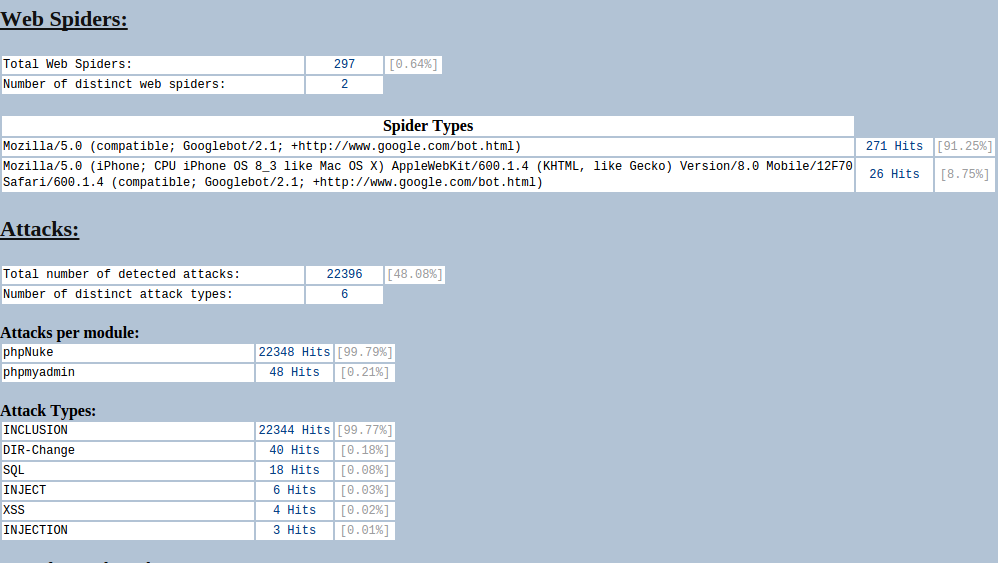
*Στην πρώτη εικόνα* μπορούμε να διακρίνουμε το σύνολο των επιθέσεων που δέχτηκε το σύστημα μας καθώς και ποιες από αυτές ήταν από *bots* και *web spiders*. Ακόμη, φαίνεται ποιες πληροφορίες ανταλλάχθηκαν μέσω *http-get* και *http-post* καθώς και το σύνολο των διαφορετικών IPs.



*Εικόνα: Καρτέλα ‘’Statistics’’ του εργαλείου όπου εμφανίζονται πληροφορίες σχετικά με τις επιθέσεις ανά ιστοσελίδα (πηγή: Hihat)*

*Στη δεύτερη εικόνα* βλέπουμε τους διαφορετικούς *user agents* που χρησιμοποιήθηκαν για είσοδο στους ιστότοπούς μας και τις διαφορετικές επιθέσεις ανά εργαλείο.

Σε αυτό το σημείο κρίνεται απαραίτητο να αναφερθεί ότι αφού δοθεί ένα όνομα για ένα Honeypot δεν μπορεί να αλλαχθεί στη συνέχεια με τον παρών κώδικα που παρέχει το εργαλείο. Συνεπώς, για το λόγο αυτό και ο ιστότοπος με τις περισσότερες επιθέσεις που βλέπουμε στην εικόνα αυτή ονομάζεται *PHPNuke* έναντι *WordPress* που θα ήταν το λογικότερο όνομά του.



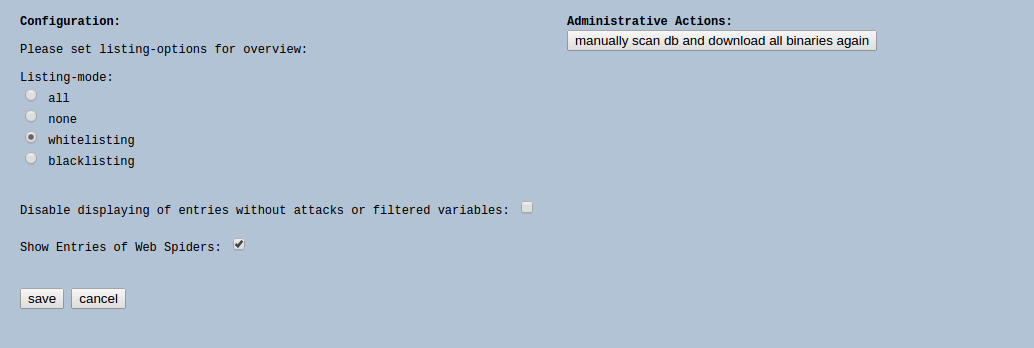
*Εικόνα: Καρτέλα ‘’Statistics’’ του εργαλείου όπου εμφανίζονται πληροφορίες σχετικά τους διαφορετικούς τύπους επιθέσεων (πηγή: Hihat)*

Στην *τρίτη εικόνα* διακρίνουμε αναλυτικότερες πληροφορίες σχετικά με τις *Web spiders - bots* που επισκέφτηκαν τους ιστότοπούς μας, καθώς και στοιχεία αναφορικά με το πλήθος των επιθέσεων και των τύπο τους που πραγματοποιήθηκαν στις ιστοσελίδες μας.

Οι τύποι αυτοί των επιθέσεων ανταποκρίνονται σε αυτούς που αναλύθηκαν στο πρώτο κομμάτι της εργασίας μας

Διαμόρφωση ρυθμίσεων – Configuration

Εδώ δίνεται η δυνατότητα διαμόρφωσης σημαντικών ρυθμίσεων, όπως αν θέλουμε να εμφανίζονται όλες οι IPs ή αν επιθυμούμε να γίνουν blacklist κάποιες από αυτές. Επίσης, μπορούμε να απενεργοποιήσουμε την εμφάνιση IDs όπου δε γίνεται κάποια επίθεση και να απενεργοποιήσουμε την εμφάνιση επισκέψεων / επιθέσεων από Web spiders.



*Εικόνα: Καρτέλα ‘’Configuration’’ του εργαλείου όπου εμφανίζονται πληροφορίες σχετικά με τις ρυθμίσεις (πηγή: Hihat)*

Συμπεράσματα

Με βάση τα παραπάνω προέκυψε ότι το εργαλείο Hihat, ανταποκρίθηκε πλήρως στις δυνατότητες που αναφέρονταν στην ιστοσελίδα του. Συνοπτικά τα πλεονεκτήματα και τα μειονεκτήματά του αναλύονται ως εξής:

**Πλεονεκτήματα**

1. Το εργαλείο παρέχει μία εξαιρετικά χρήσιμη και εύχρηστη διαδικτυακή διεπαφή στην οποία εμφανίζονται όλες οι απαραίτητες πληροφορίες σχετικά με τον επιτιθέμενο
2. Δίνεται η δυνατότητα έρευνας των επιθέσεων με σύντομο και αποτελεσματικό τρόπο
3. Παρέχεται καρτέλα γεωεντοπισμού με σκοπό το γεωγραφικό εντοπισμό των επιθέσεων
4. Ένα μέρος των ρυθμίσεων παρέχεται μέσω της διαδικτυακής διεπαφής
5. Εντοπισμός και διαχωρισμός επιθέσεων και επισκέψεων που προέρχονται από ανθρώπους και από μηχανές (bots, google crawler)

**Μειονεκτήματα**

1. Απαιτεί ένα σημαντικό χρονικό διάστημα για την παραμετροποίησή του
2. Λόγω του χρόνου που δεν έχει αναβαθμιστεί εξ ’ολοκλήρου το εργαλείο, πρέπει να χρησιμοποιηθούν παλαιότερες τεχνολογίες, όπως η έκδοση Linux 12.04, για να υποστηρίζονται όλες οι λειτουργίες του
3. Λόγω του παραπάνω, απαιτείται η γνώση κώδικα PHP και JavaScript για να είναι δυνατή η συμβατοποίησή του με κάποιες από τις νεότερες τεχνολογίες, όπως το σύγχρονο Google Maps API

**Βιβλιογραφία**

1. Digital Ocean. How to install Linux, Apache, MySQL, PHP (LAMP) stack on Ubuntu. Διαθέσιμο στο: <https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-ubuntu> [Πρόσβαση 25 Φεβρουαρίου 2016]
2. Digital Ocean. How to install and secure PHPMyAdmin on Ubuntu 12.04.

Διαθέσιμο στο: <https://www.digitalocean.com/community/tutorials/how-to-install-and-secure-phpmyadmin-on-ubuntu-12-04> [Πρόσβαση 25 Φεβρουαρίου 2016]

1. Digital Ocean. How to install Java on Ubuntu with Apt – Get.

Διαθέσιμο στο: <https://www.digitalocean.com/community/tutorials/how-to-install-java-on-ubuntu-with-apt-get> [Πρόσβαση 25 Φεβρουαρίου 2016]

1. WordPress.org. Release Archive. Διαθέσιμο στο: <https://wordpress.org/download/release-archive/> [Πρόσβαση 25 Φεβρουαρίου 2016]
2. Hihat. HIHAT Installation-Guide. Διαθέσιμο στο: <http://hihat.sourceforge.net/installation.html> [Πρόσβαση 25 Φεβρουαρίου 2016]
3. Ip2location. IP2LOCATION LITE. Διαθέσιμο στο: <http://lite.ip2location.com/>

[Πρόσβαση 25 Φεβρουαρίου 2016]