Hacking Articles

Raj Chandel's Blog

Hack the Defense Space VM (CTF Challenge)

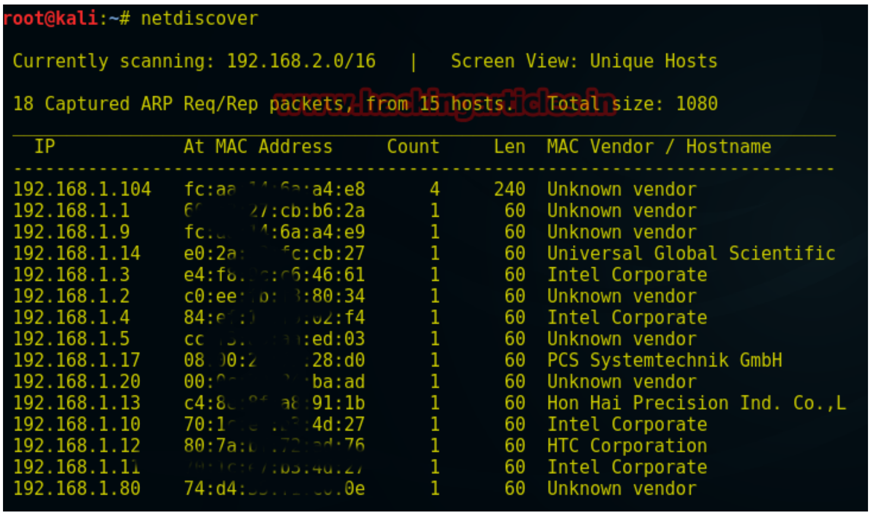
posted in CTF CHALLENGES , KALI LINUX , PENETRATION TESTING on MAY 3, 2017 by RAJ CHANDEL

SHARE

Defence VM is made by Silex Secure team. This VM is designed to honor and pay respects to the military of Nigeria and the soldiers who stood up against the terrorist attack. It is of intermediate level and is very handy in order to brush up your skills as a penetration tester. You can download it from **https://www.vulnhub.com/entry/defence-space-ctf-2017,179/**

Are you ready for the challenge soldier? First step to attack is to identify the target. So, identify your target. To identify the target we will use the following command:

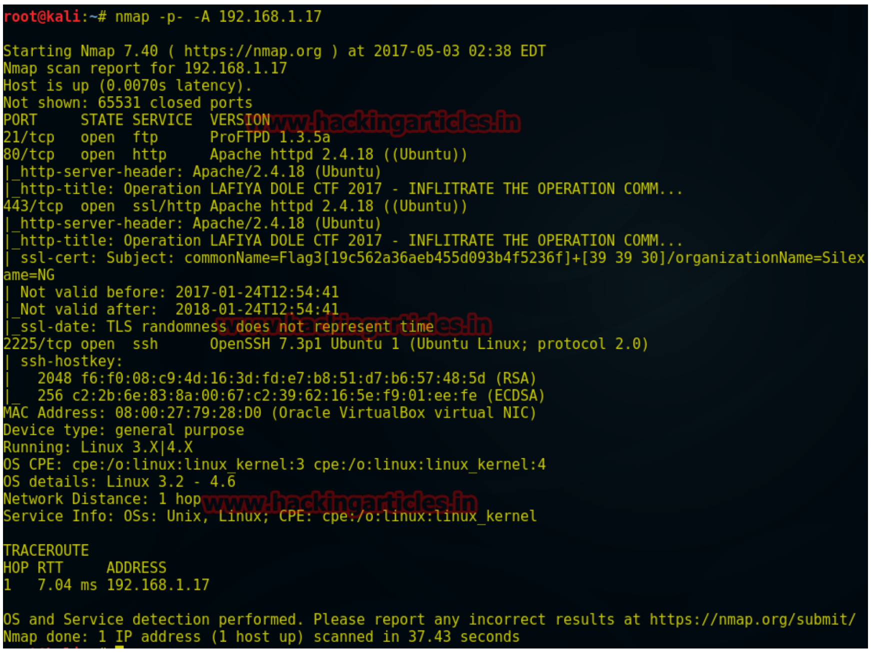
netdiscover



```
root@kali:~# netdiscover

 Currently scanning: 192.168.2.0/16   |   Screen View: Unique Hosts

 18 Captured ARP Req/Rep packets, from 15 hosts.   Total size: 1080
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.104   fc:aa[redacted]a4:e8      4     240  Unknown vendor
 192.168.1.1     6[redacted]27:cb:b6:2a    1      60  Unknown vendor
 192.168.1.9     fc[redacted]:6a:a4:e9     1      60  Unknown vendor
 192.168.1.14    e0:2a[redacted]c:cb:27    1      60  Universal Global Scientific
 192.168.1.3     e4:f8[redacted]6:46:61    1      60  Intel Corporate
 192.168.1.2     c0:ee[redacted]:80:34     1      60  Unknown vendor
 192.168.1.4     84:e[redacted]02:f4       1      60  Intel Corporate
 192.168.1.5     cc[redacted]:ed:03        1      60  Unknown vendor
 192.168.1.17    08[redacted]:28:d0        1      60  PCS Systemtechnik GmbH
 192.168.1.20    00:[redacted]ba:ad        1      60  Unknown vendor
 192.168.1.13    c4:8[redacted]:91:1b      1      60  Hon Hai Precision Ind. Co.,L
 192.168.1.10    70:1[redacted]:4d:27      1      60  Intel Corporate
 192.168.1.12    80:7a[redacted]76         1      60  HTC Corporation
 192.168.1.11    [redacted]:27             1      60  Intel Corporate
 192.168.1.80    74:d4[redacted]0e         1      60  Unknown vendor
```

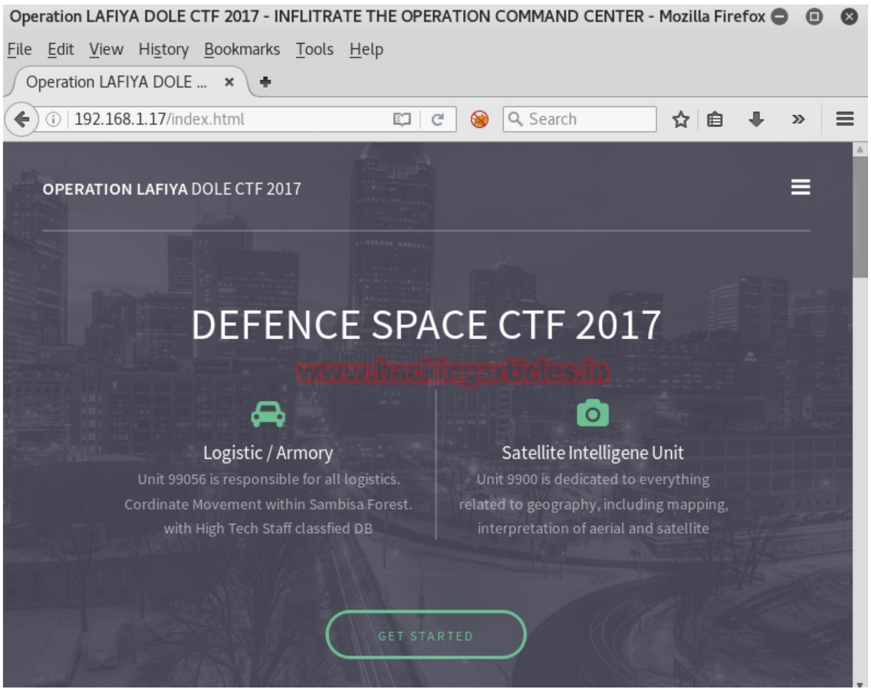
Now that you have identify your target (mine is **192.168.1.17**) you will need to acquire it and declare you victory. In order to acquire it we will need a plan to enter our enemy. To let us search for all the doors, closed or not. And for that let’s fire up the nmap.

nmap -p- -A 192.168.1.17



```
root@kali:~# nmap -p- -A 192.168.1.17

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-03 02:38 EDT
Nmap scan report for 192.168.1.17
Host is up (0.0070s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      ProFTPD 1.3.5a
80/tcp   open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Operation LAFIYA DOLE CTF 2017 - INFLITRATE THE OPERATION COMM...
443/tcp  open  ssl/http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Operation LAFIYA DOLE CTF 2017 - INFLITRATE THE OPERATION COMM...
| ssl-cert: Subject: commonName=Flag3[19c562a36aeb455d093b4f5236f]+[39 39 30]/organizationName=Silex
ame=NG
| Not valid before: 2017-01-24T12:54:41
|_Not valid after:  2018-01-24T12:54:41
|_ssl-date: TLS randomness does not represent time
2225/tcp open  ssh      OpenSSH 7.3p1 Ubuntu 1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f6:f0:08:c9:4d:16:3d:fd:e7:b8:51:d7:b6:57:48:5d (RSA)
|_  256 c2:2b:6e:83:8a:00:67:c2:39:62:16:5e:f9:01:ee:fe (ECDSA)
MAC Address: 08:00:27:79:28:D0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   7.04 ms 192.168.1.17

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 37.43 seconds
```

Our search has led us to the result that Port nos. 21, 80,443, 2225 is open with the services of FTP, HTTP, HTTPS, SSH respectively. As the port 80 is open we can open our target IP in the browser.



Operation LAFIYA DOLE CTF 2017 - INFLITRATE THE OPERATION COMMAND CENTER - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Operation LAFIYA DOLE ...
192.168.1.17/index.html
Search
OPERATION LAFIYA DOLE CTF 2017
GET STARTED

DEFENCE SPACE CTF 2017

Logistic / Armory

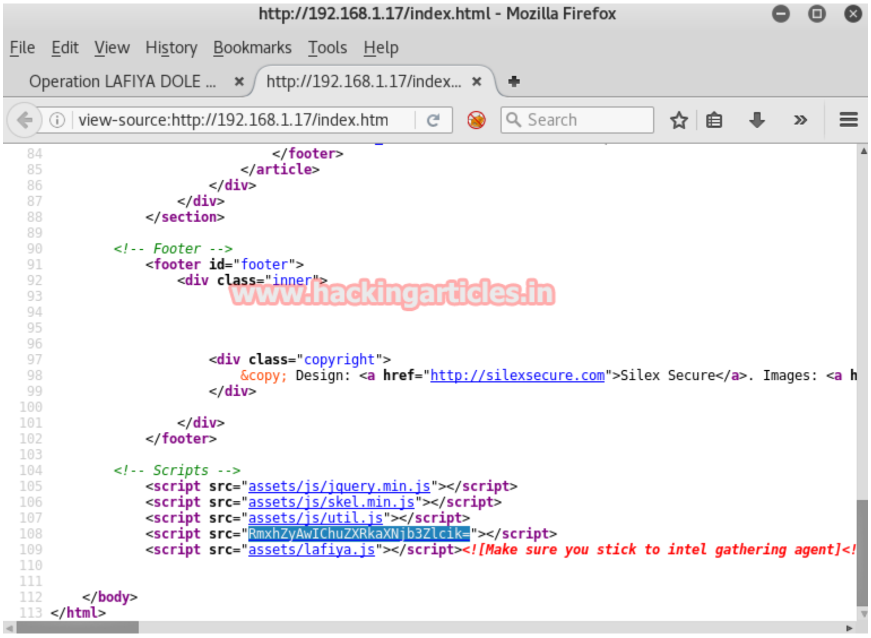
Unit 99056 is responsible for all logistics. Cordinate Movement within Sambisa Forest. with High Tech Staff classfied DB

Satellite Intelligene Unit

Unit 9900 is dedicated to everything related to geography, including mapping, interpretation of aerial and satellite

But there is no hint or what-so-ever in there. But as this based on military aspects the hint could be camouflaged.

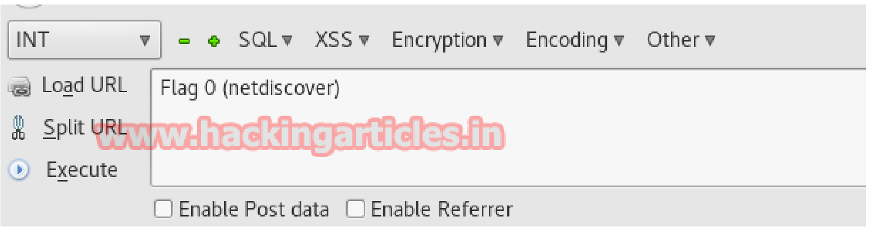
Therefore let’s check the source code.



http://192.168.1.17/index.html - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Operation LAFIYA DOLE ...
http://192.168.1.17/index...
view-source:http://192.168.1.17/index.htm
Search

```
                    </footer>
                </article>
            </div>
        </div>
    </section>

    <!-- Footer -->
        <footer id="footer">
            <div class="inner">




                <div class="copyright">
                    &copy; Design: <a href="http://silexsecure.com">Silex Secure</a>. Images: <a h
                </div>

            </div>
        </footer>

    <!-- Scripts -->
        <script src="assets/js/jquery.min.js"></script>
        <script src="assets/js/skel.min.js"></script>
        <script src="assets/js/util.js"></script>
        <script src="RmxhZyAwIChuZXRkaXNjb3Zlcik="></script>
        <script src="assets/lafiya.js"></script><![Make sure you stick to intel gathering agent]<!


    </body>
</html>
```

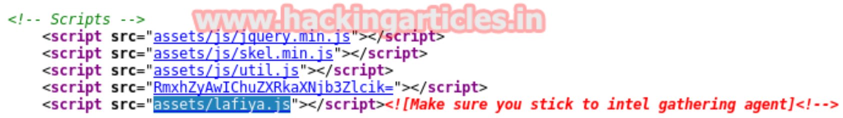
And yes!! We have found the flag 0 although it is coded□ base64. Upon decoding it will become **netdiscover.**



Flag 0 (netdiscover)

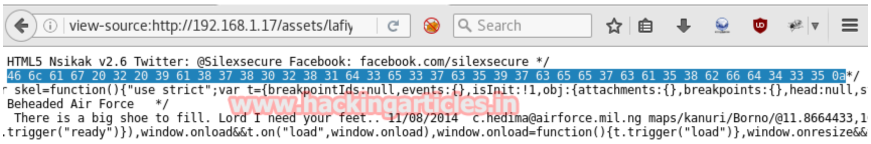
☐ Enable Post data ☐ Enable Referrer

As the source is unknown territory, I inspected more and found that there was a directory which proved to be very useful : **assests/lafiya.js□**



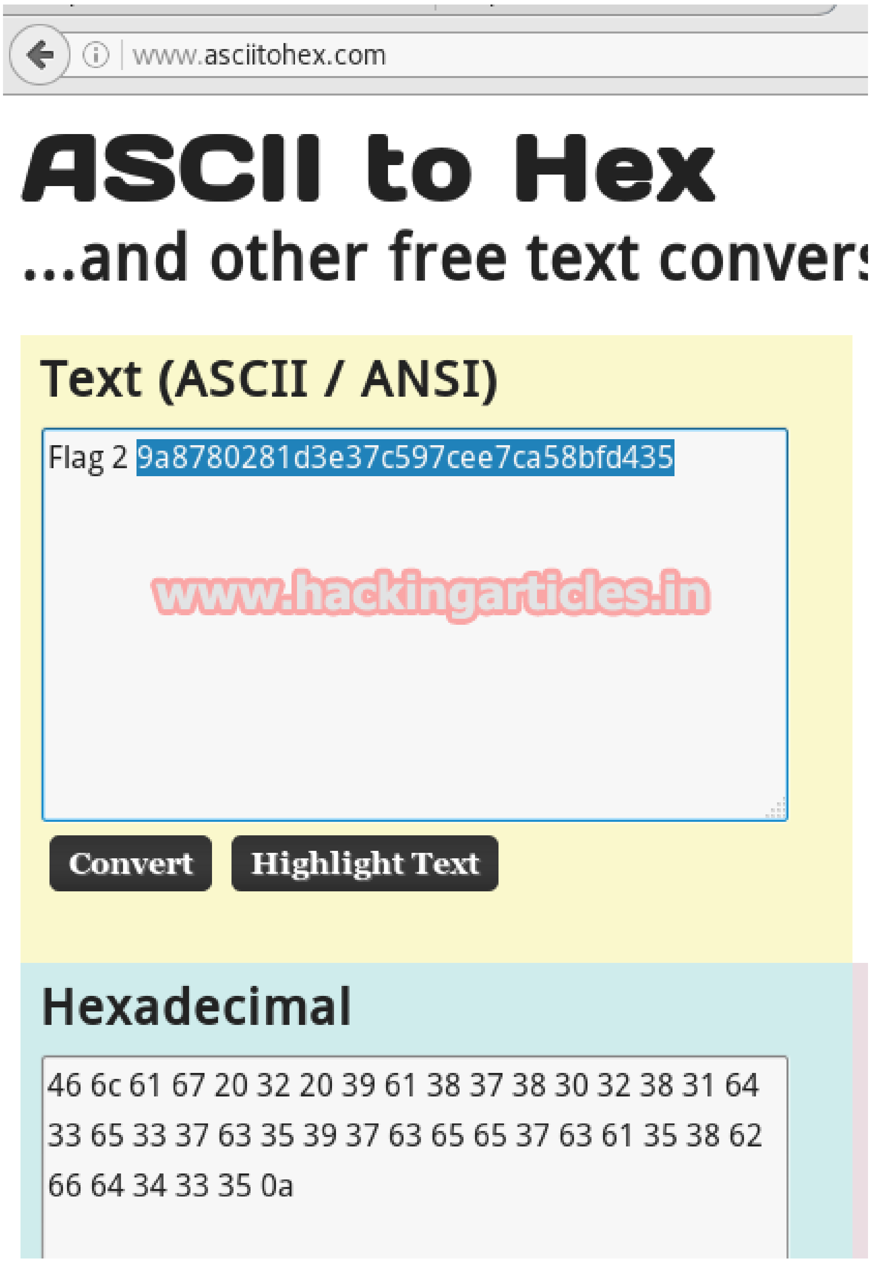
```
<!-- Scripts -->
    <script src="assets/js/jquery.min.js"></script>
    <script src="assets/js/skel.min.js"></script>
    <script src="assets/js/util.js"></script>
    <script src="RmxhZyAwIChuZXRkaXNjb3Zlcik="></script>
    <script src="assets/lafiya.js"></script><![Make sure you stick to intel gathering agent]<!-->
```

Open the said directory in browser and check it source code. In the source code you will find flag 1 which will be in□ hex.



```
HTML5 Nsikak v2.6 Twitter: @Silexsecure Facebook: facebook.com/silexsecure */
46 6c 61 67 20 32 20 39 61 38 37 38 30 32 38 31 64 33 65 33 37 63 35 39 37 63 65 65 37 63 61 35 38 62 66 64 34 33 35 0a*/
r skel=function(){"use strict";var t={breakpointIds:null,events:{},isInit:!1,obj:{attachments:{},breakpoints:{},head:null,s
Beheaded Air Force   */
 There is a big shoe to fill. Lord I need your feet.. 11/08/2014  c.hedima@airforce.mil.ng maps/kanuri/Borno/@11.8664433,1
.trigger("ready")}),window.onload&&t.on("load",window.onload),window.onload=function(){t.trigger("load")},window.onresize&&
```

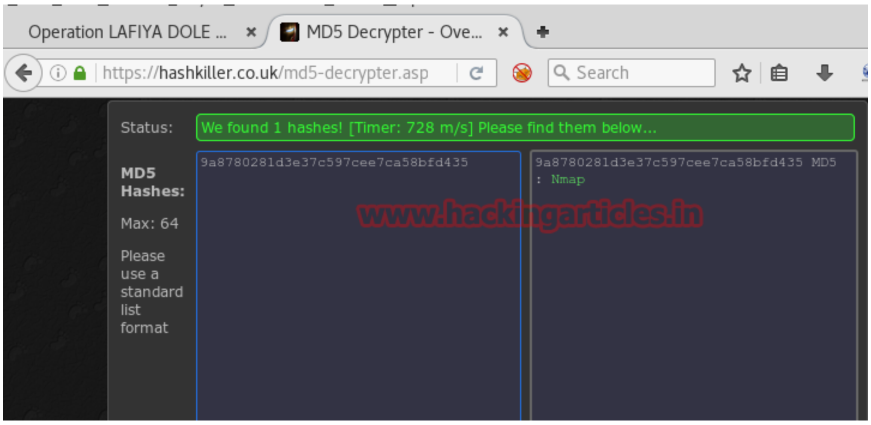
Upon converting hex you will uncover flag 2 in an MD5□ form.



```
Flag 2 9a8780281d3e37c597cee7ca58bfd435
```

```
46 6c 61 67 20 32 20 39 61 38 37 38 30 32 38 31 64
33 65 33 37 63 35 39 37 63 65 65 37 63 61 35 38 62
66 64 34 33 35 0a
```

When you convert MD5 value to its original, it will be**nmap** as shown in the image below.



Operation LAFIYA DOLE ...
MD5 Decrypter - Ove...
https://hashkiller.co.uk/md5-decrypter.asp
Search

Status: We found 1 hashes! [Timer: 728 m/s] Please find them below...

MD5 Hashes:

Max: 64

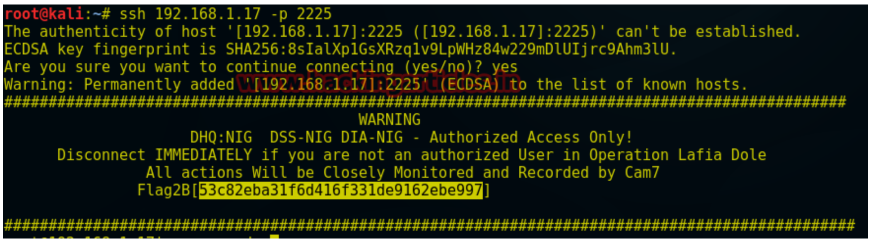
Please use a standard list format

```
9a8780281d3e37c597cee7ca58bfd435
```

```
9a8780281d3e37c597cee7ca58bfd435 MD5
: Nmap
```

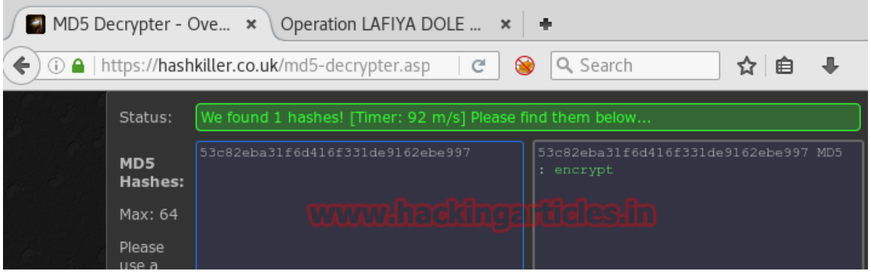
The second flag was nmap that means there is something□ the nmap that we missed. And upon reviewing it I remembered that SSH service was open on the port 2225. And so I accessed it with the following command.

ssh 192.168.1.17 –p 2225



```
root@kali:~# ssh 192.168.1.17 -p 2225
The authenticity of host '[192.168.1.17]:2225 ([192.168.1.17]:2225)' can't be established.
ECDSA key fingerprint is SHA256:8sIalXp1GsXRzq1v9LpWHz84w229mDlUIjrc9Ahm3lU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[192.168.1.17]:2225' (ECDSA) to the list of known hosts.
###############################################################################################
                                        WARNING
                     DHQ:NIG  DSS-NIG DIA-NIG - Authorized Access Only!
      Disconnect IMMEDIATELY if you are not an authorized User in Operation Lafia Dole
                All actions Will be Closely Monitored and Recorded by Cam7
               Flag2B[53c82eba31f6d416f331de9162ebe997]

################################################################################################
```

And there we have it our flag 2B in an MD5 value. Let's□ convert it.



MD5 Decrypter - Ove...
Operation LAFIYA DOLE ...
https://hashkiller.co.uk/md5-decrypter.asp
Search

Status: We found 1 hashes! [Timer: 92 m/s] Please find them below...

MD5 Hashes:

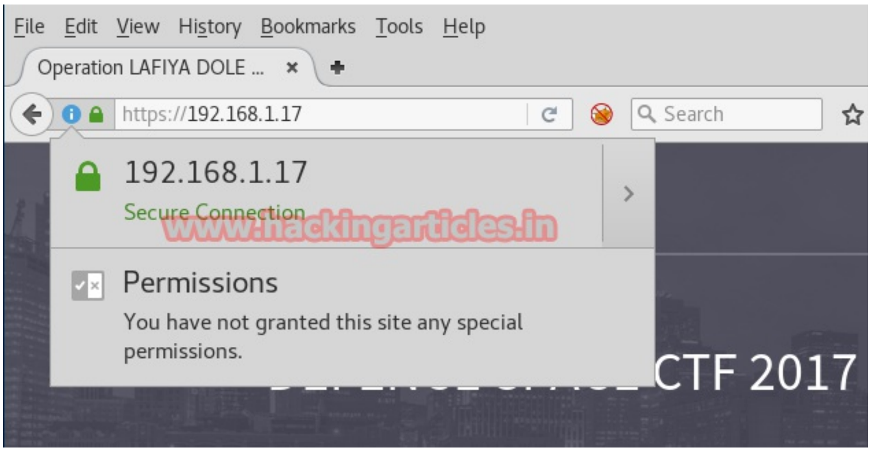
Max: 64

Please use a

```
53c82eba31f6d416f331de9162ebe997
```

```
53c82eba31f6d416f331de9162ebe997 MD5 : encrypt
```

Our flag 2B is **encrypt**. That means there is something related to encryption and security. Now the best way to provide security to a website is through it security certificate. Let's check it out.□



File Edit View History Bookmarks Tools Help
Operation LAFIYA DOLE ...
https://192.168.1.17
Search
CTF 2017

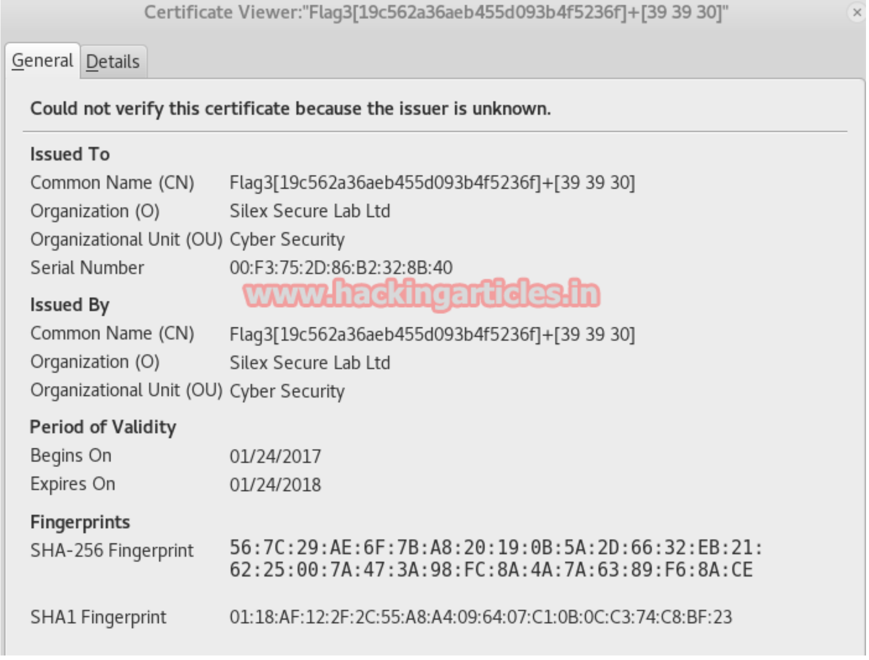
192.168.1.17

Secure Connection

Permissions

You have not granted this site any special permissions.

Now, upon examining the certificate, you will find your third□ flag and a hint i.e [39 39 30].□


Certificate Viewer:"Flag3[19c562a36aeb455d093b4f5236f]+[39 39 30]"

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN) Flag3[19c562a36aeb455d093b4f5236f]+[39 39 30]
Organization (O) Silex Secure Lab Ltd
Organizational Unit (OU) Cyber Security
Serial Number 00:F3:75:2D:86:B2:32:8B:40

Issued By

Common Name (CN) Flag3[19c562a36aeb455d093b4f5236f]+[39 39 30]
Organization (O) Silex Secure Lab Ltd
Organizational Unit (OU) Cyber Security

Period of Validity

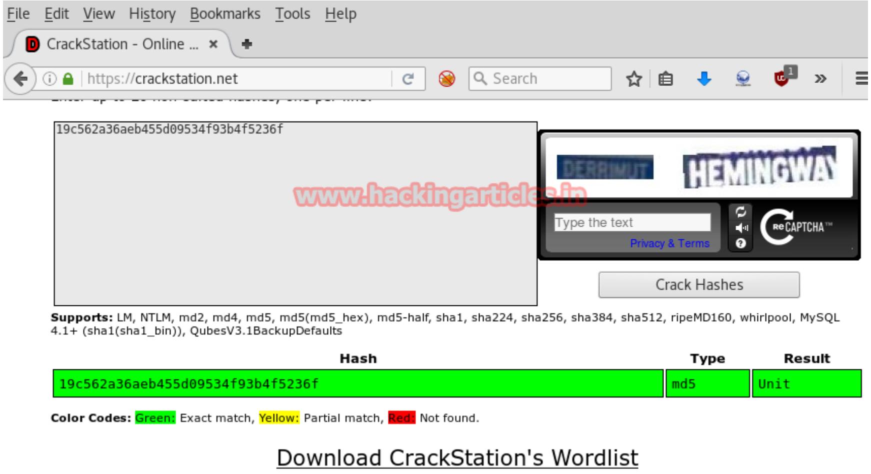
Begins On 01/24/2017
Expires On 01/24/2018

Fingerprints

SHA-256 Fingerprint 56:7C:29:AE:6F:7B:A8:20:19:0B:5A:2D:66:32:EB:21:
62:25:00:7A:47:3A:98:FC:8A:4A:7A:63:89:F6:8A:CE

SHA1 Fingerprint 01:18:AF:12:2F:2C:55:A8:A4:09:64:07:C1:0B:0C:C3:74:C8:BF:23

Firstly, decode the flag which will be **Unit**. Now if you decode it anywhere you will not get a result. And I did searched and re-searched but couldn't get it to decode. So I visited the author's walkthrough and there it says that it is translated to unit. And therefore I use unit in my walkthrough.



19c562a36aeb455d09534f93b4f5236f

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

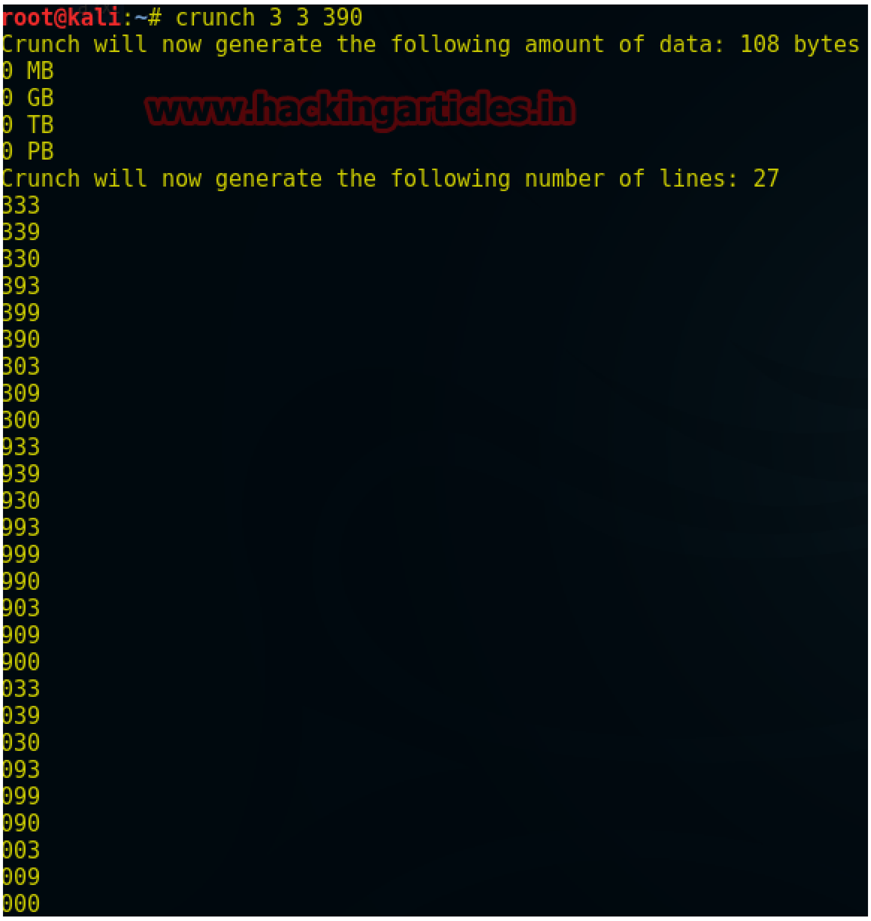
Hash	Type	Result
19c562a36aeb455d09534f93b4f5236f	md5	Unit

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

The combination of 3, 9, 0 will be the suffix of the word□ unit. But there are a lot of combination foe it so let's create those combinations with the help of crunch with command:

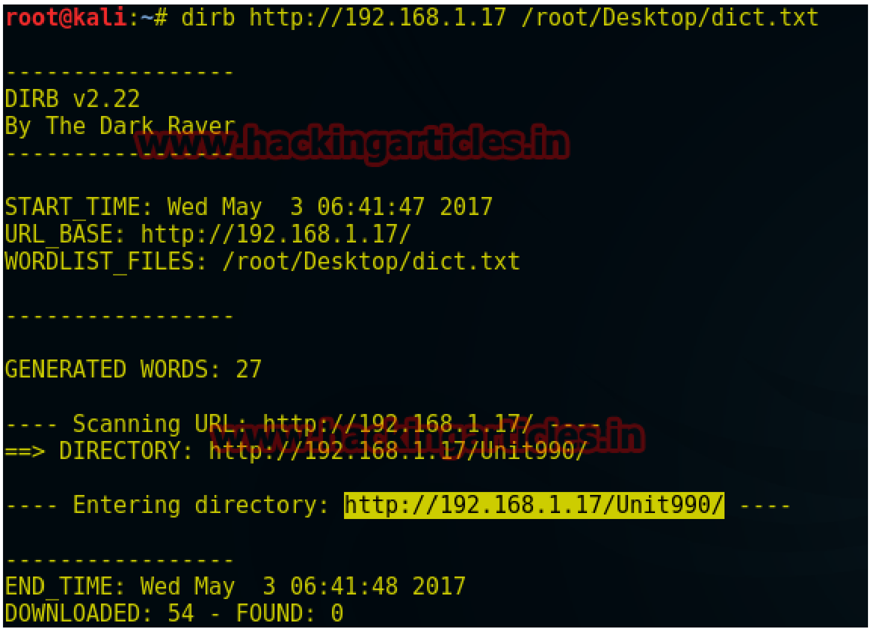
crunch 3 3 390



```
root@kali:~# crunch 3 3 390
Crunch will now generate the following amount of data: 108 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 27
333
339
330
393
399
390
303
309
300
933
939
930
993
999
990
903
909
900
033
039
030
093
099
090
003
009
000
```

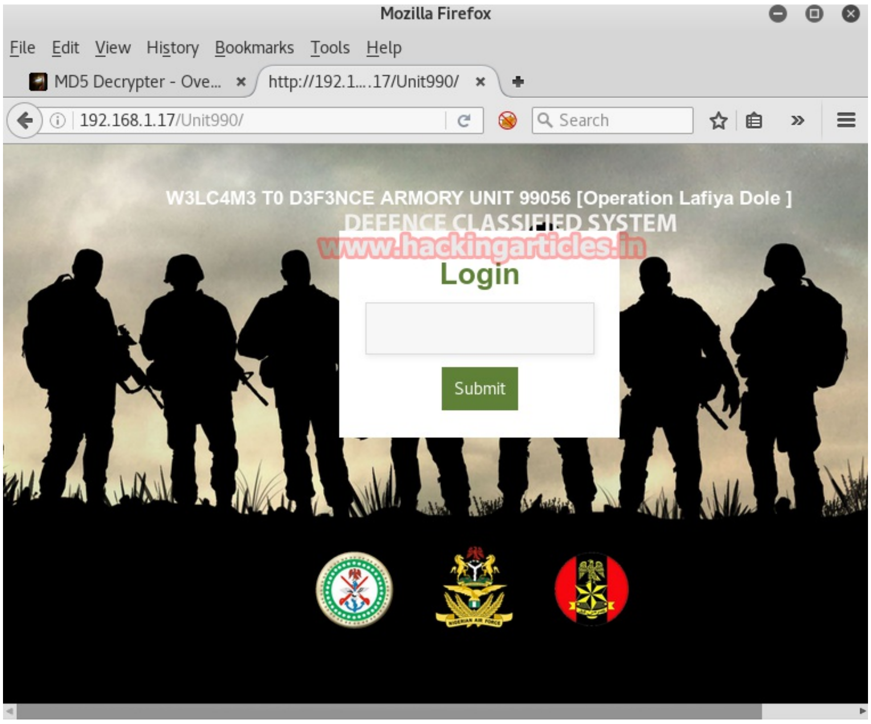
We will get 27 possible combinations and so make a text file for dictionary attack and add the word ‘unit’ as a prefix□ to every combination. Now let’s use dirb to find anything□ related to unit and these combinations.

dirb http://192.168.1.17 /rot/Desktop/dict.txt

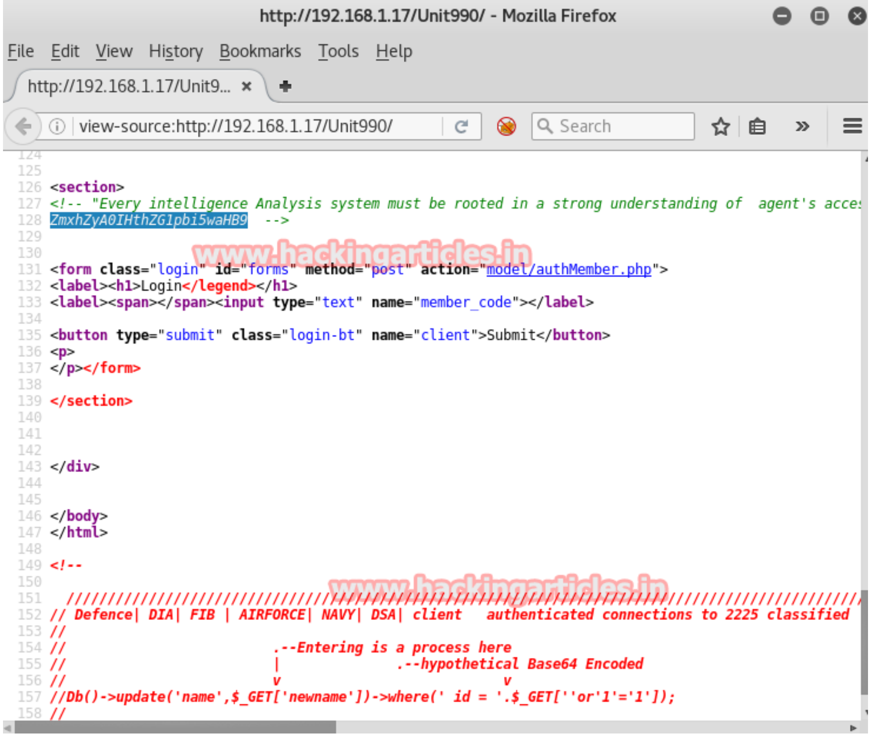


```
root@kali:~# dirb http://192.168.1.17 /root/Desktop/dict.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed May  3 06:41:47 2017
URL_BASE: http://192.168.1.17/
WORDLIST_FILES: /root/Desktop/dict.txt

-----------------

GENERATED WORDS: 27

---- Scanning URL: http://192.168.1.17/ ----
==> DIRECTORY: http://192.168.1.17/Unit990/

---- Entering directory: http://192.168.1.17/Unit990/ ----

-----------------
END_TIME: Wed May  3 06:41:48 2017
DOWNLOADED: 54 - FOUND: 0
```

To our joy there is a directory that goes by**unit990.** Let’s open it in our browser without further delay.

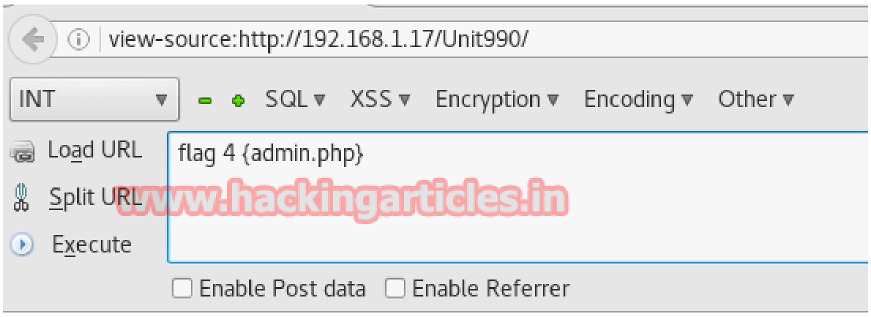

Mozilla Firefox
File Edit View History Bookmarks Tools Help
MD5 Decrypter - Ove...
http://192.1....17/Unit990/
192.168.1.17/Unit990/
Search
W3LC4M3 T0 D3F3NCE ARMORY UNIT 99056 [Operation Lafiya Dole]
DEFENCE CLASSIFIED SYSTEM
Login
Submit

We do not have credentials for logging in. So, I checked it source code instead. In the source code you will find flag 4□ in a base64 code.


http://192.168.1.17/Unit990/ - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.17/Unit9...
view-source:http://192.168.1.17/Unit990/
Search

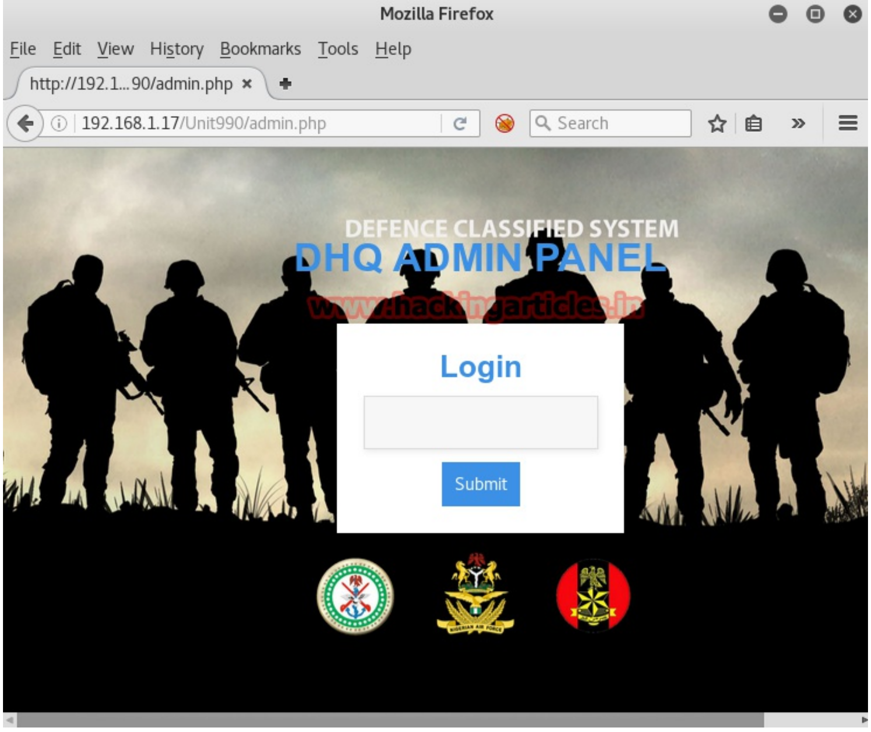
```
<section>
<!-- "Every intelligence Analysis system must be rooted in a strong understanding of  agent's acce
ZmxhZyA0IHthZG1pbi5waHB9  -->


<form class="login" id="forms" method="post" action="model/authMember.php">
<label><h1>Login</legend></h1>
<label><span></span><input type="text" name="member_code"></label>

<button type="submit" class="login-bt" name="client">Submit</button>
<p>
</p></form>

</section>



</div>


</body>
</html>

<!--

  //////////////////////////////////////////////////////////////////////////////////////////////////
// Defence| DIA| FIB | AIRFORCE| NAVY| DSA| client   authenticated connections to 2225 classified
//
//                          .--Entering is a process here
//                          |               .--hypothetical Base64 Encoded
//                          v                              v
//Db()->update('name',$_GET['newname'])->where(' id = '.$_GET[''or'1'='1']);
//
```

Decode the flag and you will get □**admin.php**

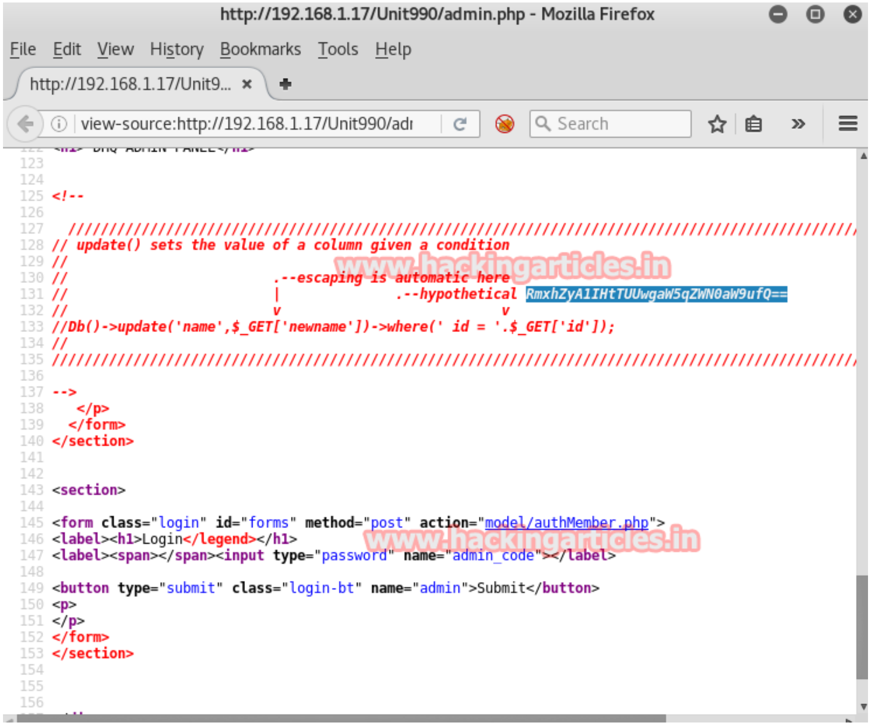


flag 4 {admin.php}

□ Enable Post data □ Enable Referrer

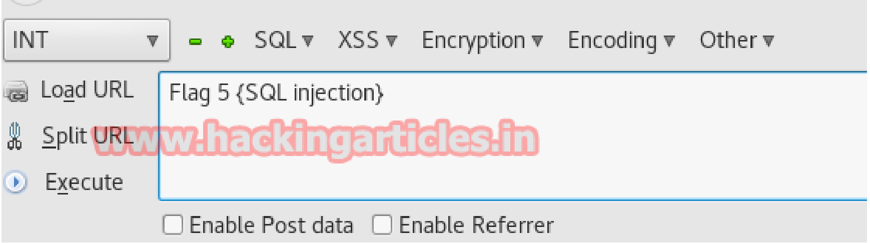

Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.1...90/admin.php
192.168.1.17/Unit990/admin.php
Search
DEFENCE CLASSIFIED SYSTEM
DHQ ADMIN PANEL
Login
Submit

Opening the previously found directory in the browser will show the same page but its source code is edited. As you will check it, you will find that flag 5 again in base64 code.


http://192.168.1.17/Unit990/admin.php - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.17/Unit9...
view-source:http://192.168.1.17/Unit990/adı
Search

```
<!--

  //////////////////////////////////////////////////////////////////////////////////////////
// update() sets the value of a column given a condition
//
//                           .--escaping is automatic here
//                           |               .--hypothetical RmxhZyA1IHtTUUwgaW5qZWN0aW9ufQ==
//                           v                    v
//Db()->update('name',$_GET['newname'])->where(' id = '.$_GET['id']);
//
//////////////////////////////////////////////////////////////////////////////////////////

-->
   </p>
  </form>
</section>


<section>

<form class="login" id="forms" method="post" action="model/authMember.php">
<label><h1>Login</legend></h1>
<label><span></span><input type="password" name="admin_code"></label>

<button type="submit" class="login-bt" name="admin">Submit</button>
<p>
</p>
</form>
</section>
```

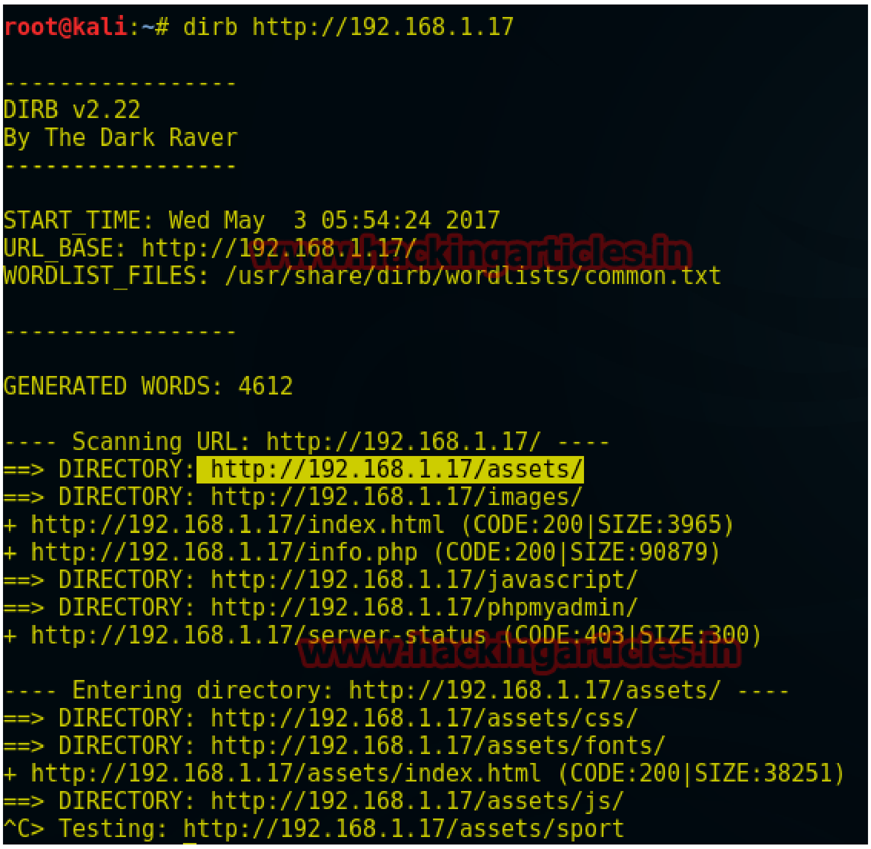
By decoding flag 5 you will get SQL injection. That means next step should be SQL injection.



Flag 5 {SQL injection}

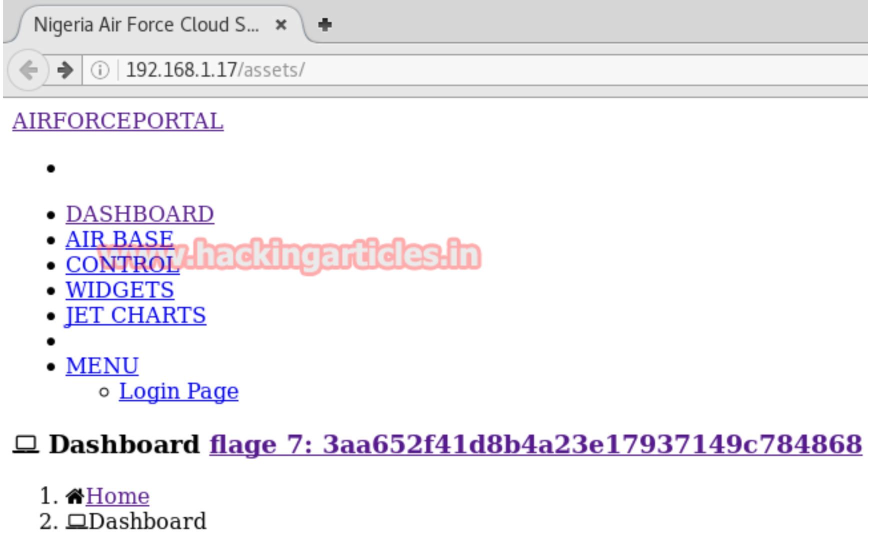
Now this hint is just to throw us of our track. I used every SQL injection technique I could find but it didn't help. So I used dirb on the target.

dirb http://192.168.1.17



```
root@kali:~# dirb http://192.168.1.17

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed May  3 05:54:24 2017
URL_BASE: http://192.168.1.17/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.17/ ----
==> DIRECTORY: http://192.168.1.17/assets/
==> DIRECTORY: http://192.168.1.17/images/
+ http://192.168.1.17/index.html (CODE:200|SIZE:3965)
+ http://192.168.1.17/info.php (CODE:200|SIZE:90879)
==> DIRECTORY: http://192.168.1.17/javascript/
==> DIRECTORY: http://192.168.1.17/phpmyadmin/
+ http://192.168.1.17/server-status (CODE:403|SIZE:300)

---- Entering directory: http://192.168.1.17/assets/ ----
==> DIRECTORY: http://192.168.1.17/assets/css/
==> DIRECTORY: http://192.168.1.17/assets/fonts/
+ http://192.168.1.17/assets/index.html (CODE:200|SIZE:38251)
==> DIRECTORY: http://192.168.1.17/assets/js/
^C> Testing: http://192.168.1.17/assets/sport
```

I found a directory called assets. And opened it in the browser and found the 7th flag.



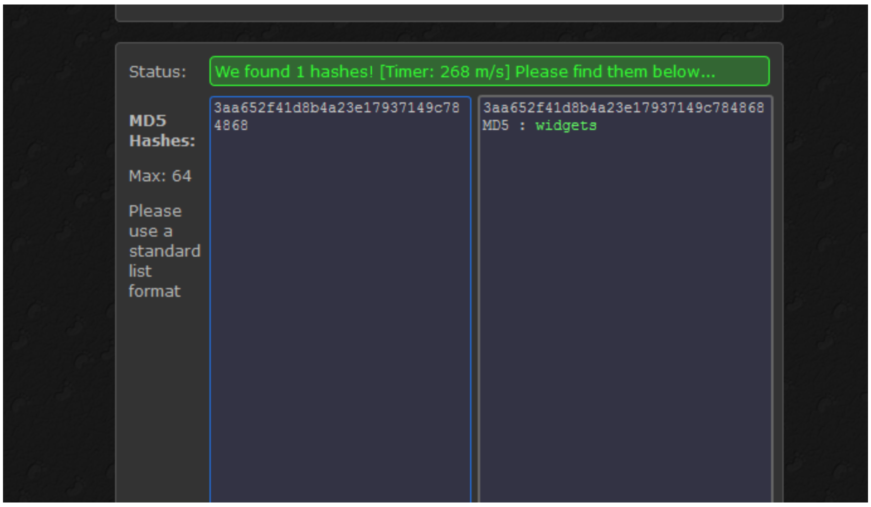
AIRFORCEPORTAL

- DASHBOARD
- AIR BASE
- CONTROL
- WIDGETS
- JET CHARTS
- MENU
  - Login Page

Dashboard flage 7: 3aa652f41d8b4a23e17937149c784868

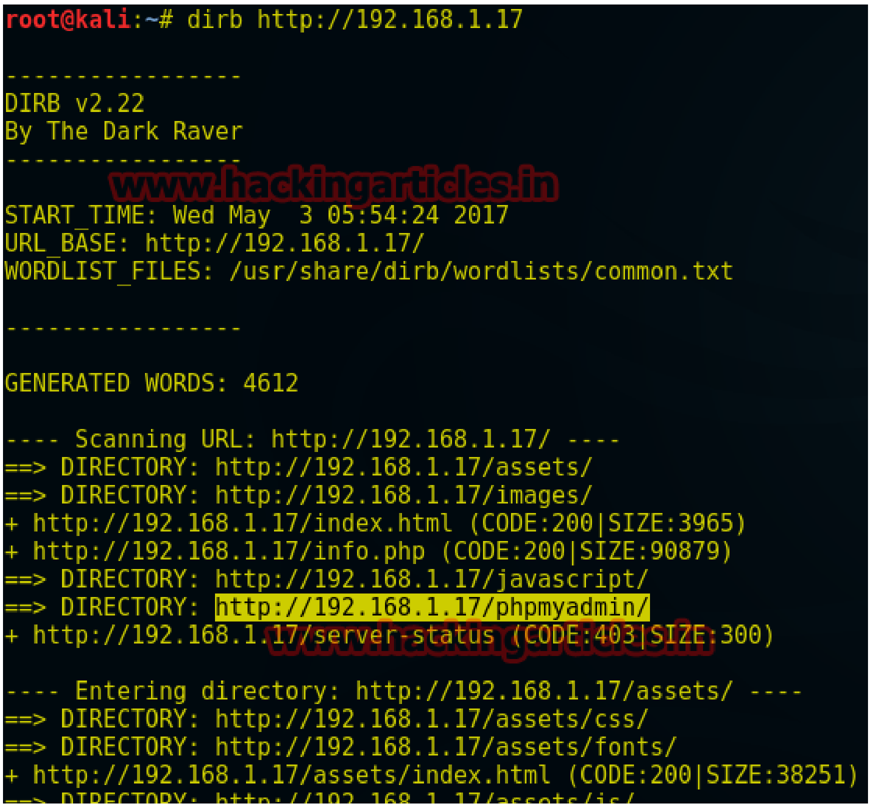
1. Home
2. Dashboard

Now try and decode it widgets.



```
Status:    We found 1 hashes! [Timer: 268 m/s] Please find them below...

MD5        3aa652f41d8b4a23e17937149c78      3aa652f41d8b4a23e17937149c784868
Hashes:    4868                              MD5 : widgets

Max: 64

Please
use a
standard
list
format
```

Now you can try and decode it but it’s hopeless to decode it anywhere online. So examined the dirb result more and found another directory called **phpmyadmin**



```
root@kali:~# dirb http://192.168.1.17

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed May  3 05:54:24 2017
URL_BASE: http://192.168.1.17/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.17/ ----
==> DIRECTORY: http://192.168.1.17/assets/
==> DIRECTORY: http://192.168.1.17/images/
+ http://192.168.1.17/index.html (CODE:200|SIZE:3965)
+ http://192.168.1.17/info.php (CODE:200|SIZE:90879)
==> DIRECTORY: http://192.168.1.17/javascript/
==> DIRECTORY: http://192.168.1.17/phpmyadmin/
+ http://192.168.1.17/server-status (CODE:403|SIZE:300)

---- Entering directory: http://192.168.1.17/assets/ ----
==> DIRECTORY: http://192.168.1.17/assets/css/
==> DIRECTORY: http://192.168.1.17/assets/fonts/
+ http://192.168.1.17/assets/index.html (CODE:200|SIZE:38251)
==> DIRECTORY: http://192.168.1.17/assets/js/
```

If you open this directory in browser you will find a log in□ page. I used the top 10 most commonly used password and username i.e root and root and got in. In the database I found a **silex** table. Now silex is the team’s name so I guess this is most important table.

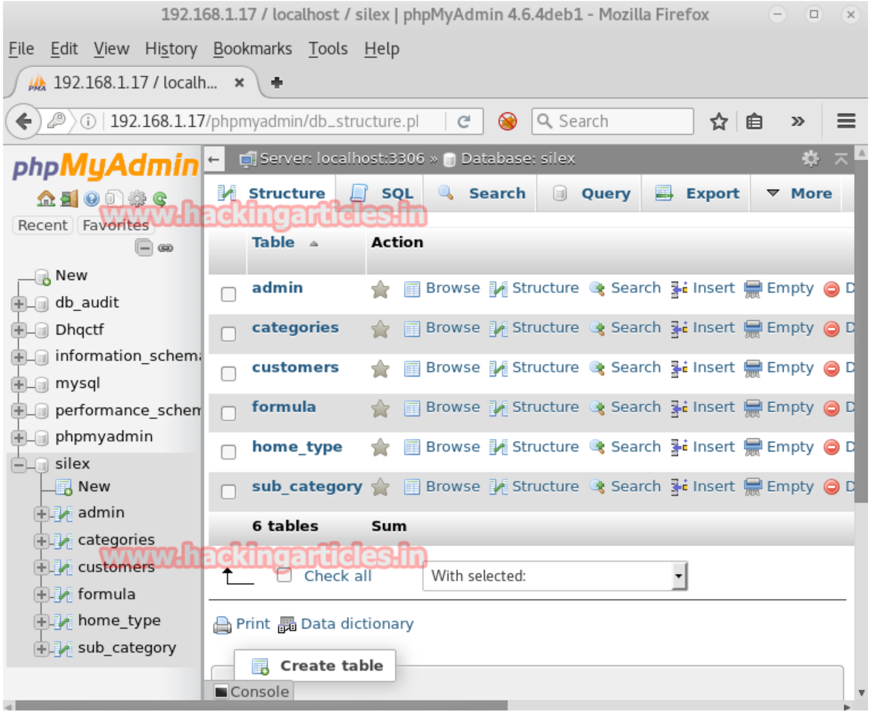
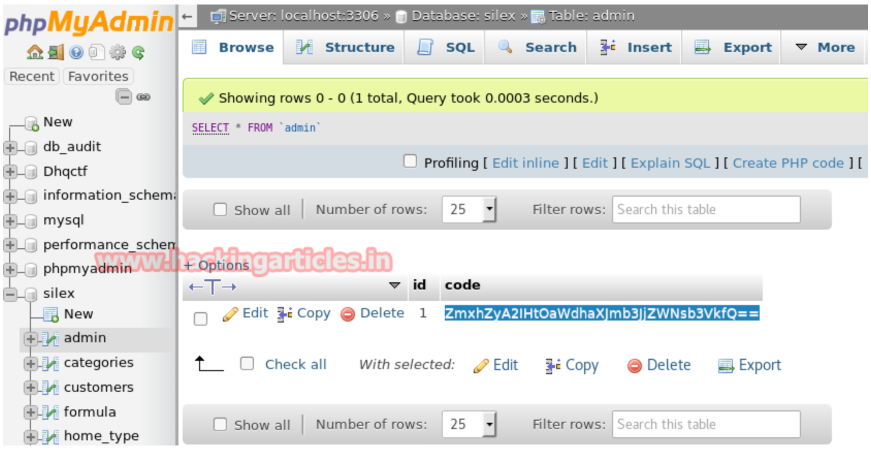


Table	Action
admin	Browse Structure Search Insert Empty D
categories	Browse Structure Search Insert Empty D
customers	Browse Structure Search Insert Empty D
formula	Browse Structure Search Insert Empty D
home_type	Browse Structure Search Insert Empty D
sub_category	Browse Structure Search Insert Empty D
6 tables	Sum

Upon checking it, I found admin and in admin there was our 6th flag coded in base64□



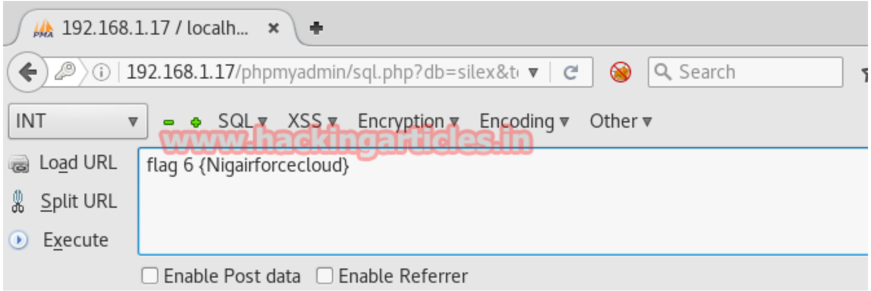
phpMyAdmin
Server: localhost:3306 » Database: silex » Table: admin
Browse Structure SQL Search Insert Export More
Recent Favorites
New
db_audit
Dhqctf
information_schema
mysql
performance_schema
phpmyadmin
silex
New
admin
categories
customers
formula
home_type
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [
Show all
Number of rows: 25
Filter rows: Search this table
+ Options
Check all
With selected: Edit Copy Delete Export
www.hackingarticles.in

Showing rows 0 - 0 (1 total, Query took 0.0003 seconds.)

```
SELECT * FROM `admin`
```

	id	code
Edit Copy Delete	1	ZmxhZyA2IHtOaWdhaXJmb3JjZWNsb3VkfQ==

Upon decoding, it says **Nigiarforcecloud.**



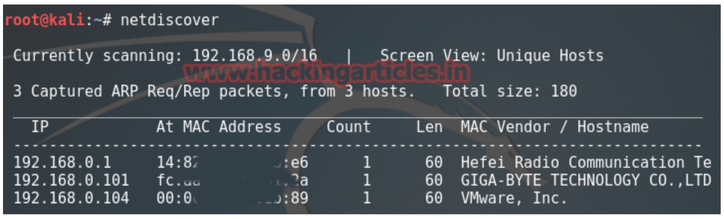
192.168.1.17 / localh...
192.168.1.17/phpmyadmin/sql.php?db=silex&t
Search
INT
SQL XSS Encryption Encoding Other
Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
www.hackingarticles.in

flag 6 {Nigairforcecloud}

And voila!! All our flags are uncovered. Good work soldiers.□ Solving this VM was good exercise and I salute the fallen Nigerian soldiers and wish them peace and praise the whole army.

Author: **Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact ~~here~~

Related

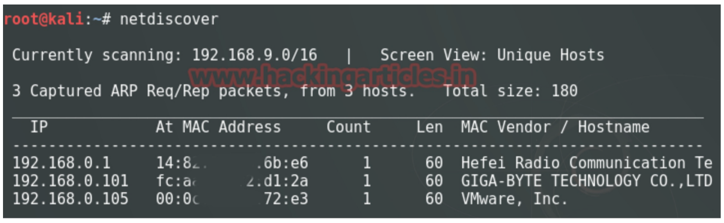


```
root@kali:~# netdiscover

 Currently scanning: 192.168.9.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.0.1     14:8[redacted]:e6      1       60  Hefei Radio Communication Te
 192.168.0.101   fc.[redacted]?a      1       60  GIGA-BYTE TECHNOLOGY CO.,LTD
 192.168.0.104   00:0[redacted]:89      1       60  VMware, Inc.
```

Hack the Simple VM (CTF Challenge)

September 7, 2016

In "CTF Challenges"

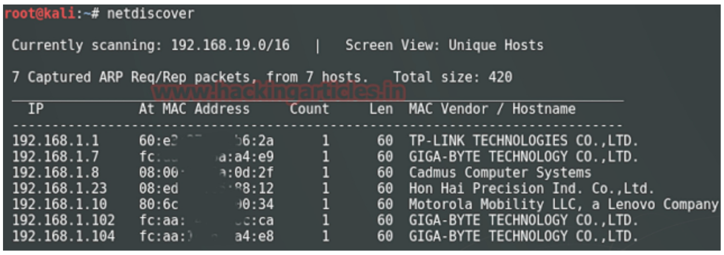


```
root@kali:~# netdiscover

 Currently scanning: 192.168.9.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.0.1     14:8[redacted].6b:e6      1       60  Hefei Radio Communication Te
 192.168.0.101   fc:a[redacted].d1:2a      1       60  GIGA-BYTE TECHNOLOGY CO.,LTD
 192.168.0.105   00:0[redacted]72:e3      1       60  VMware, Inc.
```

Hack the Milnet VM (CTF Challenge)

September 8, 2016

In "CTF Challenges"



```
root@kali:~# netdiscover

 Currently scanning: 192.168.19.0/16   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 420
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     60:e[redacted]6:2a      1       60  TP-LINK TECHNOLOGIES CO.,LTD.
 192.168.1.7     fc[redacted]a:a4:e9      1       60  GIGA-BYTE TECHNOLOGY CO.,LTD.
 192.168.1.8     08:00[redacted]:0d:2f      1       60  Cadmus Computer Systems
 192.168.1.23    08:ed[redacted]8:12      1       60  Hon Hai Precision Ind. Co.,Ltd.
 192.168.1.10    80:6c[redacted]0:34      1       60  Motorola Mobility LLC, a Lenovo Company
 192.168.1.102   fc:aa:[redacted]c:ca      1       60  GIGA-BYTE TECHNOLOGY CO.,LTD.
 192.168.1.104   fc:aa:[redacted]a4:e8      1       60  GIGA-BYTE TECHNOLOGY CO.,LTD.
```

Hack the Zorz VM (CTF Challenge)

December 16, 2016

In "CTF Challenges"

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← HOW TO USE PUBLIC IP ON KALI LINUX

Leave a Reply

Enter your comment here...

Search

ENTER KEYWORD

Subscribe to Blog via Email

Email Address

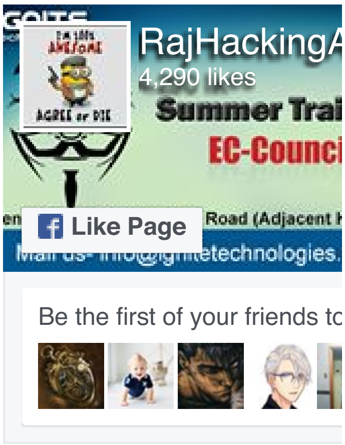
SUBSCRIBE

Categories

- BackTrack 5 Tutorials
- Batch File Tricks
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Dll File Hacking
- Domain Hacking
- Email Hacking
- Face Book Hacking
- Footprinting
- Google Hacking
- Hacking Tools
- Internet
- Kali Linux
- Others
- Penetration Testing

- Registry Tricks
- Social Engineering Toolkit
- Software
- Trojans & Backdoors
- Uncategorized
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking

Facebook Page



RajHackingA

4,290 likes

Like Page

Be the first of your friends tc

Share