

# D0Not5top Vulnhub's vulnerable lab challenge

#### Information Security Inc.



## Contents

- About Vulnhub
- Target VM
- Test Setup
- Walkthrough
- References

## **About Vulnhub**

 To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration





## **Target VM**

- Target VM: D0Not5top
- Download the ova file https://download.vulnhub.com/d0not5top/D0Not5top\_3mrgnc3\_v1.2.ova
- Import the ova file into your favorite hypervisor
  - D0Not5top\_3mrgnc3\_v1.2.ova
- Attach a DHCP enable vmnet to the machine and run it
- Objective
   Find the flags





© Testing environment

Linux Kali (attacker) >>> Firewall >>> D0Not5top (target vm)



© From the attacker machine run the following command to find out Target VMs IP address:

| root@LUCKY64:-#    | netdiscover -i eth  | 2 -r 192.1<br>Screen | 168.254.0<br>View: Unique Hosts |
|--------------------|---------------------|----------------------|---------------------------------|
| Sufference y South | - /- · · ·          | bereen               |                                 |
| 4 Captured ARP     | Req/Rep packets, f  | rom 4 host           | ts. Total size: 240             |
| IP                 | At MAC Address      | Count                | Len MAC Vendor / Hostname       |
| 192.168.254.1      | 00:50:56:c0:00:08   |                      | 60 Unknown vendor               |
| 192.168.254.2      | 00:50:56:ef:1d:d2   | 1                    | 60 Unknown vendor               |
| 192.168.254.139    | 00:0c:29:e8:2d:87   | 1                    | 60 Unknown vendor               |
| 192.168.254.254    | 4 00:50:56:e5:db:b1 | 1                    | 60 Unknown vendor               |

© Scan the target machine IP (192.168.254.139)

| root | LOLUCI | KY64 | 4:~  | ŧ.,  | /Scan. | pγ |
|------|--------|------|------|------|--------|----|
| ТСР  | port   | 22   | is   | ope  | en     |    |
| TCP  | port   | 25   | is   | ope  | en     |    |
| ТСР  | port   | 53   | is   | ope  | en     |    |
| ТСР  | port   | 80   | is   | ope  | en     |    |
| ТСР  | port   | 111  | l is | s or | ben    |    |
| TCP  | port   | 332  | 265  | is   | open   |    |



#### ◎ Use dirb tool to scan the web application

| reotgLUCRY64:-# dirb http://192.168.254.139 /usr/share/wordlists/dirb/big.txt |
|---|
|   |
| DTRB v2.22  |
| By The Dark Raver   |
|   |
| START TIME: Thu Sep / 20:09:25 201/   |
| URL BASE: http://192.168.254.139/   |
| WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt                             |
|   |
|   |
| GENERATED WORDS: 20458  |
| Scanning URL: http://192.168.254.139/   |
| > DIRECTORY: hLLp://192.168.254.139/archive/                                  |
| > DIRECTORY: http://192.168.254.139/blackhole/                                |
| > DIRECTORY: hllp://192.168.254.139/blog/                                     |
| > DIRECTORY: http://192.168.254.139/control/                                  |
| ==> DIRECTORY: http://192.168.254.139/dropbox/                                |
| > DIRECTORY: http://192.168.254.139/extend/                                   |
| ==> DIRECTORY: http://192.168.254.139/fccd/                                   |
| => DIRECTORY: http://192.168.254.139/gamea/                                   |
| > DIRECTORY: http://192.168.254.139/mint/                                     |
| ==> DIRECTORY: http://192.168.254.139/phpmyadmin/                             |
| > DIRECTORY: http://192.168.254.139/plugins/                                  |
| > DIRECTORY: http://192.106.254.139/search/                                   |
| + hLtp://192.168.254.139/server-status (CODE:403 512E:222)                    |
| > DIRECTORY: http://192.168.254.139/support/                                  |
| ==> DIRECTORY: http://192.168.254.139/Lag/                                    |
| > DIRECTORY: http://192.168.254.139/thackback/                                |
| ==> DIRECTORY: http://192.168.254.139/wp-admin/                               |
| > DIRECTORY: http://192.168.254.139/wp-content/                               |
| ==> DIRECTORY: http://192.168.254.139/wp-includes/                            |
| Entering directory: http://192.168.254.139/archive/                           |
| > DIRECTORY: http://192.168.254.139/archive/admin/                            |
| Set of the disert state http://102.102.064-120/blashbala/                     |
| ===> Directory: http://192.168.254.139/blackhole/admin/                       |
|   |
| Entering directory: http://192.168.254.139/blog/                              |
| > DIRECTORY: http://192.168.254.139/blog/admin/                               |
| Entering directory: http://192.168.254.139/contact/                           |
| > DIRECTORY: http://192.168.254.139/contact/admin/                            |
| Balanian di malana bilan (/192 102 254 120/malan1/                            |
| + http://192.168.254.139/control/LICENSE (CODE:2001SIZE:11436)                |
| > DTRECTORY: http://192.168.254.139/control/css/                              |
| ==> DIRECTORY: http://192.168.254.139/control/fonts/                          |
| > DIRECTORY: DILD://192.108.254.139/CONTROL/18/                               |



© Explore http://192.168.254.139/control/ using curl

root@LUCKY64: # curl -iv http://192.168.254.139/control/
\* Trying 192.168.254.139...
\* Connected to 192.168.254.139 (192.168.254.139) port 80 (#0)
> GET /control/ HTTP/1.1
> Host: 192.168.254.139

#### ○ Capture the flag

<div id="wrapper">
 <!-- FL46 1:urh8fu3i039rfoy254sx2xtrs5wc6767w -->
 <nav class="navbar navbar-inverse navbar-fixed-top" role="navigation">



#### © Explore http://192.168.254.139/control/js/ using curl

|   | ot@LUCKY64:-# cu: | rl -iv  | http:  | //192 | .168.2 | 254.139/ | contro | o1/ | js/ |
|---|-------------------|---------|--------|-------|--------|----------|--------|-----|-----|
| * | Trying 192.168    | .254.13 | 39     |       |        |          |        |     |     |
| * | Connected to 192  | .168.25 | 54.139 | (192  | .168.2 | 254.139) | port   | 80  | (#0 |
| > | GET /control/js/  | HTTP/1  | .1     |       |        |          |        |     |     |
| > | Host: 192.168.25  | 4.139   |        |       |        |          |        |     |     |

#### Found a Readme file (README.MadBro)





© Using curl to access <u>http://192.168.254.139/control/js/README.MadBro</u> reveals another flag encoded in binary

Encoded Flag > FL101110\_10:1111010111011r10101 0q10svdfsxk1001i111ry100f10srtr110 0010h10

Decoded Flag > FL46\_2:30931r42q2svdfsxk9i13ry4f2 srtr98h2

: # curl -iv http://192.168.254.139/control/js/README.MadBro Trying 192.168.254.139... Connected to 192.168.254.139 (192.168.254.139) port 80 (#0) GET /control/js/README.MadBro HTTP/1.1 Host: 192.168.254.139 HTTP/1.1 200 OK TTP/1.1 200 OK Date: Fri, 08 Sep 2017 09:43:05 GMT ate: Fri, 08 Sep 2017 09:43:05 GMT Server: Apache erver: Apache Last-Modified: Mon, 03 Apr 2017 16:17:14 GMT ast-Modified: Mon, 03 Apr 2017 16:17:14 GMT Accept-Ranges: bytes ccept-Ranges: bytes Content-Length: 544 ontent-Length: 544 MadBro MadBro MadBro MadBro MadBro MadBro MadBro M4K3 5UR3 2 S3TUP YOUR /3TC/H05T5 N3XT T1M3 L0053R... 1T'5 D0Not5topMe.ctf !!!! 1M 00T4 H33R.. MadBro MadBro MadBro MadBro MadBro MadBro MadBro 



◎ Verify open TCP port 25

| root | LOLUCI | KY 64 | 1:   | # ./ | /Scan | .py |
|------|--------|-------|------|------|-------|-----|
| TCP  | port   | 22    | is   | ope  |       |     |
| TCP  | port   | 25    | is   | ope  |       |     |
| TCP  | port   | 53    | is   | ope  |       |     |
| TCP  | port   | 80    | is   | ope  | en    |     |
| TCP  | port   | 11:   | l i: | s op | ben   |     |
| TCP  | port   | 332   | 265  | is   | open  |     |

© Found a HexCode which can be converted to ASCII HexCode => 46 4c 34 36 5f 33 3a 32 396472796 63637756 8656874 327231646434 717070756 5793437 347 3767879610a



◎ After converting the code (using rax2), another flag is revealed

root@LUCKY64: # rax2 -s "46 4c 34 36 5f 33 3a 32 396472796 63637756 8656874 327231646434 717070756 5793437 347 3767879610a' FL46 3:29drvf67uheht2r1dd4gppuev474svxva



© The following page has a message written in leet (https://en.wikipedia.org/wiki/Leet )

| root@Scapy:-/leetspea        | # python3 leet.py "M4K3 5UR3 2 S3TUP YOUR 3TC H05T5 N3XT T1M3 L0053R 1T5 D0Not5topMe.ctf"  |
|------------------------------|--|
| make sure are setup v        | nur etc hosts next time looser its   |
| make bare are beedp y        | vot to hole to here time for the state of th |
|                              | * Trying 192.168.254.139   |
|                              | * Connected to 192.168.254.139 (192.168.254.139) port 80 (#0)  |
|                              | > GET /control/js/README.MadBro HTTP/1.1   |
|                              | > Host: 192.168.234.139  |
| Encoded Message => M4K3      | > Accept: */*  |
| 5UR3 2 S3TUP YOUR            | < HTTP/1.1 200 OK  |
| /3TC/H05T5 N3XT T1M3         | HTTP/1.1 200 OK<br>< Date: Fri, 08 Sep 2017 09:43:05 GMT   |
|                              | Date: Fri, 08 Sep 2017 09:43:05 GMT  |
| L0053R 1T'5                  | < Server: Apache   |
| DONIALEtan Maratt IIII       | Server, apache<br>< Last-Modified: Mon. 03 Apr 2017 16:17:14 GMT   |
|                              | Last-Modified: Mon, 03 Apr 2017 16:17:14 GMT   |
|                              | < ETag: "220-54c457e101a40"  |
|                              | ETag: "220-54c457e101a40"  |
| > Decoded Message =>         | < Accept-Ranges: bytes   |
|                              | < Content-Lenath: 544  |
| make sure are setup your etc | Content-Length: 544  |
| booto povit timo loggar ita  |  |
|                              | <  |
| D0Not5tonMe.ctf              | ≰ MadRro MadRro MadRro MadRro MadRro MadRro MadRro MadRro ≸  |
| Donatiotophile.oti           | # Mathis Hard 2 Satur Your / arc/hors Nature Mathis Mathis Mathis #  |
|                              | # 1T'5 DONot5topMe.ctf !!!! #  |
|                              | # 1M 00T4 H33R #   |
|                              | ♥ MadBro MadBro MadBro MadBro MadBro MadBro MadBro MadBro #  |
|                              |  |
|                              |  |

information security inc.

#### ◎ Add the host "D0Not5topMe.ctf " to /etc/hosts

| root@LUCKY64:-/ | leetspeak# cat /etc/hosts |
|-----------------|---------------------------|
| 127.0.0.1       | localhost                 |
| 127.0.1.1       | LUCKY64.rtma.tk           |
|                 |                           |
|                 |                           |
| 192.168.254.139 | D0Not5topMe.ctf           |

◎ Open D0Not5topMe.ctf in browser and click on Register

|                      |   |   |  |                    |                   | - search     |               |                          |
|----------------------|---|---|--|--------------------|-------------------|--------------|---------------|--------------------------|
| Offensive Security 🔪 | Kali Linux 🥆 Kali Docs 🛞 Kali Toc   | ols DExploit-DB Aircrack-ng   | ⊛Kali Forums ⊛NetHunter                  | Most Visited *     | ffensive Security | Kali Linux 🕚 | Kali Docs     | Kali Tools DE            |
|                      | 00000   | MegustaGameo  |  |                    |                   | <u>Geo</u>   | arch          | Q 0                      |
|                      | E Quick links @ FAQ   |   |  |                    |                   |              |               | 🕼 Register 🙂 Login       |
|                      | W Board Index   |   |  |                    |                   |              | R & currently | Fri Gep 08, 2017 3:12 pr |
|                      | FORUM   |   |  | 6                  | otres Pos         | TS LAST POS  | ir.           |                          |
|                      | ® <b>- 20</b>   | Worka Suko Gameo Di Besto<br>enay ayingbiay ucheay amengay ow<br>otay antiag away exempt dephotoay                              | ay egisitationay array edisay emay email | way ayay egualomay | 0 0               | No posite    |               |                          |
|                      |   |   |  |                    |                   |              |               |                          |
|                      | LOGIN REGISTER  |   |  |                    |                   |              |               |                          |
|                      |   | Passeore  | (Remember me                             | Lingin             |                   |              |               |                          |
|                      | LOGIN REGISTER  | Passaore  | Remember me                              | Logn               |                   |              |               |                          |
|                      | LOOM REGISTER<br>Usernane<br>In Istatuteore at subor deline - 0 reg<br>Mats Laine war safet with 2 d m 5<br>Registred Lainer, Vongelated en<br>Lagent - Advensariany, Relation  | Passente<br>pannets, 0 moden and 1 guest (based on use<br>an Apr 62, 3017 533 pm<br>ent<br>Meximum                              | Permember me []                          | Lage               |                   |              |               |                          |
|                      | LOCK ESSETER<br>Cremanni<br>WHO IS ONLINE<br>In task tear before in 1 user poster 0 neg<br>Mats users are write wat 2 a de<br>Fregeteret cases: to registerer a<br>Lighter Amountain (State das<br>BETH Days  | Passenet<br>pannet, 0 noden and 1 guest (based on use<br>in Apr 62, 3017 533 pm<br>anternation                                  | ( Planeetiber me (                       | Lage               |                   |              |               |                          |
|                      | LOOM REGETER<br>Username<br>Models Concern<br>Hassi uans are office to org<br>Argenter data and a concern<br>Argenter data and a concern<br>BRTHOLAYS<br>No Steffungs Italiay   | Passerrit<br>ganneti, 0 nodon and 1 guest (based on us<br>n år 17. 2017 533 pm<br>ans<br>ans                                    | ( Premember we )                         | Lagn               |                   |              |               |                          |
|                      | LOOM REGENTER<br>Username<br>Media Look 5 OKLME<br>Hass Looks are offen and 2 de fa<br>Hass Looks and 2 de fa<br>Hass and 2 de fa | Passent [   | (Researcher and )                        | Lagn               |                   |              |               |                          |
|                      | Loon Reaction<br>Generative<br>Web Code Mark<br>Hall and Service As a service of the service<br>Association of the service of the service of the service<br>Association of the service of the service of the service<br>Association of the service of the service of the service<br>Association of the service of the service of the service<br>Association of the service of the service of the service of the service<br>Association of the service of the  | Passend<br>parent, 1 best mit gred fabrid in se<br>and 65 2017 233 gm<br>memory<br>memory<br>nemers 1 - Our newst rember Megodi | Nanoedber ne (*                          | Logn               |                   |              |               |                          |



Explore the webpage source code and look for hidden html pages



◎ Open the hidden webpage and looks like Brainfuck encoded data

| ( d0not5topme.ctf/FLaR6yF1nD3rZ_html                                      |
|---|
| 🕅 Offensive Security 🌂 Kali Linux 🥆 Kali Docs 🛞 Kali Tools 🚺 Exploit-DB 🕴 |
| +++++ +++[- >++++ ++++< ]>+++ +++++ ,<+++ +[-><] >                        |
| ++,<+ +++++ [->++ ++++< ]>+++ ++,<+ +++++ [->< ]>, +++++                  |
| +.<++ +++++ [->++ +++++ <]>++ +.<++ +++++ [-> <]>                         |
| ++. <++++ ++[-> +++++ +<]>+ +++++ +.<++ +++[-> ++++< ]>+++ +.<++          |
| +++++ +<[>++++++ +<[>+++++++++++++++++++                                  |
| +++++ ++[-><] >, <++++ +++[- >++++<] >++++ +++++,                         |
| <++++[ -> <]>,< +++++ +++[-><]> ,+,+,,+++ ++++++                          |
| +< +++++ ++[-> +++++<]> ,++++ +.++. +++++ ++++. <+++++.                   |
| ++++[-><]>  |
| .<++++ [->++ +<]>+ +,++,,++ .++++++[ ->< ]><                              |



O Decoding the data (<u>https://www.splitbrain.org/services/ook</u>) reveals another flag





#### by click on Board Administration

| ensive Security 🌂 Kal | i Linux 🥆 Kali Docs 🛞 Kali Toi   | ols 🚺 Exploit-DB 👠 Aircrack-ng 闭               |
|-----------------------|--|--|
|                       | <b>@@@@@</b> @   | MegustaGameo<br>GameoGameo                     |
|                       | E Quick links 🛛 FAQ  |  |
|                       | # Board Index  |  |
|                       | MegustaGameo - Regi  | istration                                      |
|                       | Username:<br>Length must be between 3<br>characters and 20 characters. |  |
|                       | Email address:   |  |
|                       | Password:<br>Must be between 6 characters<br>and 100 characters.       |  |
|                       | Confirm password:  |  |
|                       | Language:  | British English                                |
|                       | My timezone:   | UTC-04:00 - 08 Sep 2017, 11:29                 |
|                       |  | America/Anguilla                               |
|                       | CONFIRMATION OF REGISTRAT  | NON  |
|                       | To prevent automated registra  | ations the board requires you to enter a confi |



Information Security Confidential - Partner Use Only

Hovering over "Board Administrator" reveales a new hidden page
 "G4M35.ctf"

|                          | please contact the | Board Administrator. |
|--------------------------|--------------------|----------------------|
|                          | Confirmation code  | :<br>Enter the       |
|                          | # Board index      |                      |
|                          |                    |                      |
|                          |                    |                      |
| mailto:Megusta@G4M35.ctf |                    |                      |



Add G4M35.ctf to /etc/hosts

| root@LUCKY64:-# | cat /etc/hosts  |
|-----------------|-----------------|
| 127.0.0.1       | localhost       |
| 127.0.1.1       | LUCKY64.rtma.tk |
|                 |                 |
| 192.168.254.139 | D0Not5topMe.ctf |
| 192.168.254.139 | G4M35.ctf       |

○ Open <u>http://G4M35</u>.ctf in a browser and use "Inspect Element" tool Select the Debugger tab. Found another link H3x6L64m3. Use dirb for further enumeration





#### © Access http:// G4M35.ctf/H3x6L64m3/textures/skybox/dawnclouds/nz.jpg



◎ The picture reveals an octal code. Decode the octal code and get another flag

Flag > FL46\_5:09k87h6g4e25gh44wa1rybyfi898hncdt

root@LUCKY64: f printf "\106\114\64\66\137\65\72\60\71\153\70\67\150\66\147\64\145\62\65\147\150\64\167\141\61\162\171\142\171\146\151\70\71\70\150\156\14 3\144\164\n" EL46 5:09k87h6g4e25gh44wa1rybyfi898hncdt



#### References

• Vulnhub website https://www.vulnhub.com

 Vulnerable VM download https://download.vulnhub.com/d0not5top/D0Not5top\_3mrgnc3\_v1.2.ova

• Leet https://en.wikipedia.org/wiki/Leet

• LeetSpeak to English convertor https://github.com/floft/leetspeak

• Brainfuck decoder https://www.splitbrain.org/services/ook

