D0Not5top Vulnhub's vulnerable lab challenge

Information Security Inc.

Contents

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

About Vulnhub

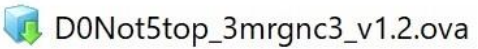
- To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration

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



- Attach a DHCP enable vmnet to the machine and run it

- Objective
Find the flags

Test Setup

◎ Testing environment

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

Walkthrough

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

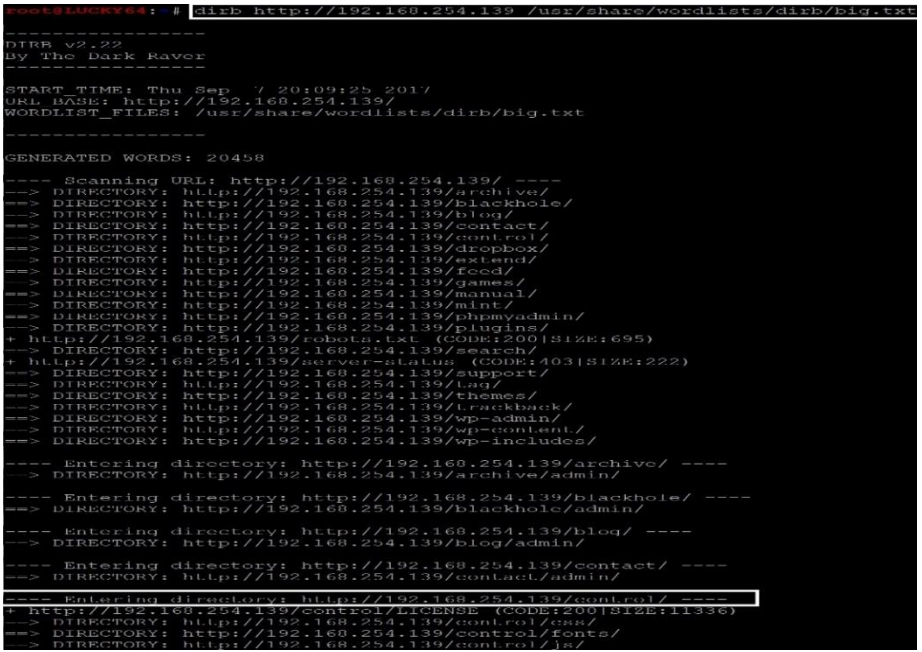
```
root@LUCKY64:~# netdiscover -i eth2 -r 192.168.254.0
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.254.1   00:50:56:c0:00:08      1      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 00:50:56:e5:db:b1      1      60  Unknown vendor
```

◎Scan the target machine IP (192.168.254.139)

```
root@LUCKY64:~# ./Scan.py
TCP port 22 is open
TCP port 25 is open
TCP port 53 is open
TCP port 80 is open
TCP port 111 is open
TCP port 33265 is open
```

Walkthrough

◎ Use dirb tool to scan the web application



Walkthrough

◎ 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">
```

Walkthrough

◎ Explore http://192.168.254.139/control/js/ using curl

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

◎ Found a Readme file (README.MadBro)

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /control/js</title>
 </head>
 <body>
<h1>Index of /control/js</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a
href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/control/">Parent Directory</a></td><td> </td><td align="right">  -
</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="README.MadBro">README.MadBro</a></td><td align="right">2017-04-03 17:17  </t
d><td align="right">544 </td><td> </td></tr>
```

Walkthrough

◎ Using curl to access http://192.168.254.139/control/js/README.MadBro reveals another flag encoded in binary

Encoded Flag >
FL101110_10:1111010111011r101010q10svdfsxk1001i111ry100f10srtr1100010h10

Decoded Flag >
FL46_2:30931r42q2svdfsxk9i13ry4f2srtr98h2

.

```
root@LUCKY64: # 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
> User-Agent: curl/7.50.1
> Accept: */*
>
< HTTP/1.1 200 OK
HTTP/1.1 200 OK
< Date: Fri, 08 Sep 2017 09:43:05 GMT
Date: Fri, 08 Sep 2017 09:43:05 GMT
< Server: Apache
Server: Apache
< 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"
< Accept-Ranges: bytes
Accept-Ranges: bytes
< Content-Length: 544
Content-Length: 544
<
############################################################
# MadBro 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 MadBro #
############################################################

                FL101110_10:111101011101
                1r101010q10svdfsxk1001i1
                11ry100f10srtr1100010h10
```

Walkthrough

◎ Verify open TCP port 25

```
root@LUCKY64:~# ./Scan.py
TCP port 22 is open
TCP port 25 is open
TCP port 53 is open
TCP port 80 is open
TCP port 111 is open
TCP port 33265 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

```
root@LUCKY64:~# telnet 192.168.254.139 25
Trying 192.168.254.139...
Connected to 192.168.254.139.
Escape character is '^]'.
220 46 4c 34 36 5f 33 3a 32 396472796 63637756 8656874 327231646434 717070756 5793437 347 3767879610a EXIM SMTP
HELO 192.168.254.239
250 DONot5top Hello 192.168.254.239 [192.168.254.128]
```

◎ 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_3:29dryf67uheht2r1dd4qppuev474svxva
```

Walkthrough

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

```
root@Scapy:~/leetspeak# python3 leet.py "M4K3 5UR3 2 S3TUP Y0UR 3TC H05T5 N3XT T1M3 L0053R 1T5 D0Not5topMe.ctf"
make sure are setup your etc hosts next time looser its
```

```
root@LUCKY64:~# 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
> User-Agent: curl/7.50.1
> Accept: */*
>
< HTTP/1.1 200 OK
HTTP/1.1 200 OK
< Date: Fri, 08 Sep 2017 09:43:05 GMT
Date: Fri, 08 Sep 2017 09:43:05 GMT
< Server: Apache
Server: Apache
< 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"
< Accept-Ranges: bytes
Accept-Ranges: bytes
< Content-Length: 544
Content-Length: 544

<
############################################################
# MadBro MadBro MadBro MadBro MadBro MadBro MadBro MadBro #
# M4K3 5UR3 2 S3TUP Y0UR /3TC/H05T5 N3XT T1M3 L0053R...   #
# 1T'5 D0Not5topMe.ctf !!!!                               #
# 1M 00T4 H33R..                                          #
# MadBro MadBro MadBro MadBro MadBro MadBro MadBro MadBro #
############################################################
```

Encoded Message => M4K3 5UR3 2 S3TUP Y0UR /3TC/H05T5 N3XT T1M3 L0053R... 1T'5 D0Not5topMe.ctf !!!!

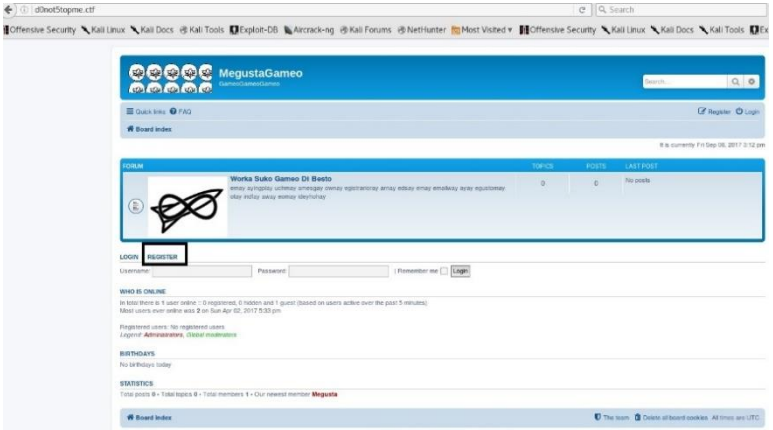
> Decoded Message => make sure are setup your etc hosts next time looser its D0Not5topMe.ctf

Walkthrough

◎ 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

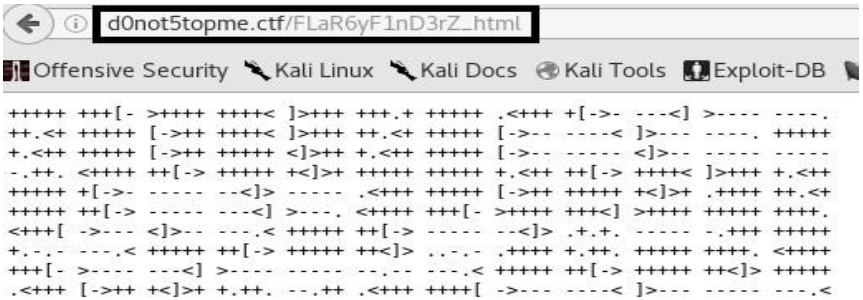


Walkthrough

◎ Explore the webpage source code and look for hidden html pages

```
<div class="panel">
    <div class="inner">
    <fieldset class="submit-buttons">
                <input type="submit" name="agreed" id="agreed" value="I agree to these terms" class="button1" /> 
        <input type="submit" name="not_agreed" value="I do not agree to these terms" class="button2" />
                <input type="hidden" name="FLaR6yF1nD3rZ_html" value="" />
```

◎ Open the hidden webpage and looks like Brainfuck encoded data



Walkthrough

◎ Decoding the data (https://www.splitbrain.org/services/ook) reveals another flag

Walkthrough

◎ Access http:// D0Not5topMe.ctf click on Register then on I Agree followed by click on Board Administration

Walkthrough

◎ Hovering over “Board Administrator” reveales a new hidden page “G4M35.ctf”

Walkthrough

◎ Add G4M35.ctf to /etc/hosts

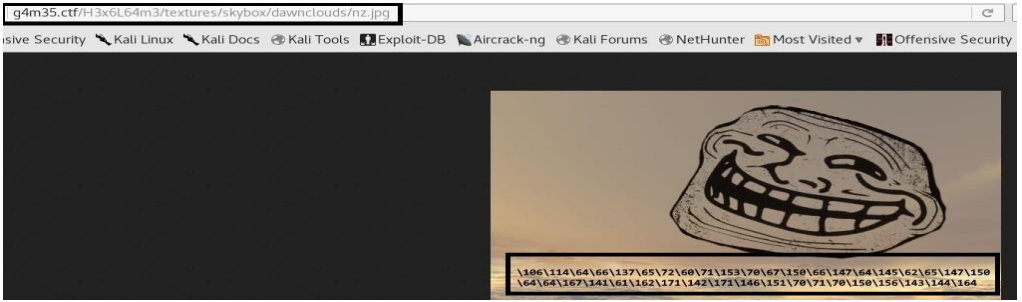
```
root@LUCKY64:~# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       LUCKY64.rtma.tk


192.168.254.139 D0Not5topMe.ctf
192.168.254.139 G4M35.ctf
```

◎ Open http://G4M35.ctf in a browser and use “Inspect Element” tool
Select the Debugger tab. Found another link H3x6L64m3.
Use dirb for further enumeration


```
root@LUCKY64:~# dirb http://g4m35.ctf/H3x6L64m3/ /usr/share/wordlists/dirb/big.txt

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

START_TIME: Fri Sep  8 03:07:59 2017
URL_BASE: http://g4m35.ctf/H3x6L64m3/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

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

GENERATED WORDS: 20458

---- Scanning URL: http://g4m35.ctf/H3x6L64m3/ ----
+ http://g4m35.ctf/H3x6L64m3/LICENSE (CODE:200|SIZE:1085)
==> DIRECTORY: http://g4m35.ctf/H3x6L64m3/audio/
==> DIRECTORY: http://g4m35.ctf/H3x6L64m3/css/
==> DIRECTORY: http://g4m35.ctf/H3x6L64m3/libs/
==> DIRECTORY: http://g4m35.ctf/H3x6L64m3/textures/
```

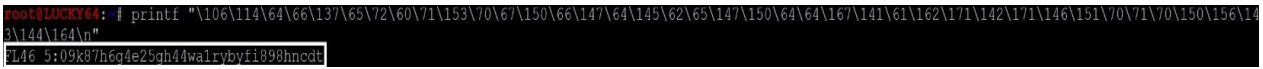
Walkthrough

◎ 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



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