

We make a file that we should secure I made it by using nano \*.txt  
Then

Changing the modes that it's not accessible to anyone but the owner which here is (m) by using chmod \*\*\* filename  
If 421 according to wrx write read and excute

Then we change the owner to the root which is not accessible to anyone but the true administrator of this device I work from

The image displays two side-by-side windows. The left window is a Kali Linux terminal running in Oracle VM VirtualBox. The right window is the Microsoft OneDrive web interface.

**Kali Linux Terminal:**

```
m@kali: ~  
$ nano topsecert_file_that_has_my_bankaccount_and_itspassword_for_no_reason.txt  
$ cat topsecert_file_that_has_my_bankaccount_and_itspassword_for_no_reason.txt  
top secret file  
you can't read this  
$ chmod 000 topsecert_file_that_has_my_bankaccount_and_itspassword_for_no_reason.txt  
$ cat topsecert_file_that_has_my_bankaccount_and_itspassword_for_no_reason.txt  
cat: topsecert_file_that_has_my_bankaccount_and_itspassword_for_no_reason.txt: Permission denied  
$ chown root topsecert_file_that_has_my_bankaccount_and_itspassword_for_no_reason.txt  
chown: changing ownership of 'topsecert_file_that_has_my_bankaccount_and_itspassword_for_no_reason.txt': Operation not permitted  
$ sudo chown root topsecert_file_that_has_my_bankaccount_and_itspassword_for_no_reason.txt  
$ cat topsecert_file_that_has_my_bankaccount_and_itspassword_for_no_reason.txt  
cat: topsecert_file_that_has_my_bankaccount_and_itspassword_for_no_reason.txt: Permission denied
```

**Microsoft OneDrive:**

The OneDrive interface shows a sidebar with navigation options: Home, My files, Shared, Favorites, Recycle bin, Browse files by, People, Meetings, and Quick access. The main area displays a list of files and a table of recent activity.

Opened	Owner	Activity
23m ago	Dr. Gamal Selim	
31m ago	Elhossiny Ibrahim	
31m ago	Elhossiny Ibrahim	

here I make a user called ali  
and gave him ownership from visudo and and wrote some comments with bash command (echo)

then if he got hacked I changed his password from 1 to 2 and went to sudoers.tmp and commented his ownership command from ali ALL=(ALL:ALL) ALL to

#ali ALL=(ALL:ALL) ALL that made him a regular user without any permissions or benefits till we recover this account to his owner

Then I switched to ali user to see if it works that show me I don't even have permission to read the directories

The image shows a Kali Linux terminal window on the left and a Microsoft OneDrive web interface on the right.

**Kali Linux Terminal:**

```
m@kali: ~  
File Actions Edit View Help  
[m@kali]-[~]  
$ sudo useradd ali  
[m@kali]-[~]  
$ sudo passwd ali  
New password:  
Retype new password:  
passwd: password updated successfully  
[m@kali]-[~]  
$ sudo visudo  
visudo: /etc/sudoers.tmp unchanged  
[m@kali]-[~]  
$ sudo visudo  
[m@kali]-[~]  
$ sudo visudo  
[m@kali]-[~]  
$ ECHO WE  
ECHO: command not found  
[m@kali]-[~]  
$ echo we made him have superuser mode  
we made him have superuser mode  
[m@kali]-[~]  
$ sudo passwd ali  
New password:  
Retype new password:  
passwd: password updated successfully  
[m@kali]-[~]  
$ echo we changed his password till we fix this  
we changed his password till we fix this  
[m@kali]-[~]  
$ touch topsecret_file_that_ali_can_access.txt  
[m@kali]-[~]  
$ chmod 700 topsecret_file_that_ali_can_access.txt  
[m@kali]-[~]  
$ su ali  
Password:  
$  
$  
$ whoami  
ali  
$ ls  
ls: cannot open directory '.': Permission denied  
$ echo i have no permission here  
i have : not found here  
$ ^[[A^[[A  
$ : 6:  
$
```

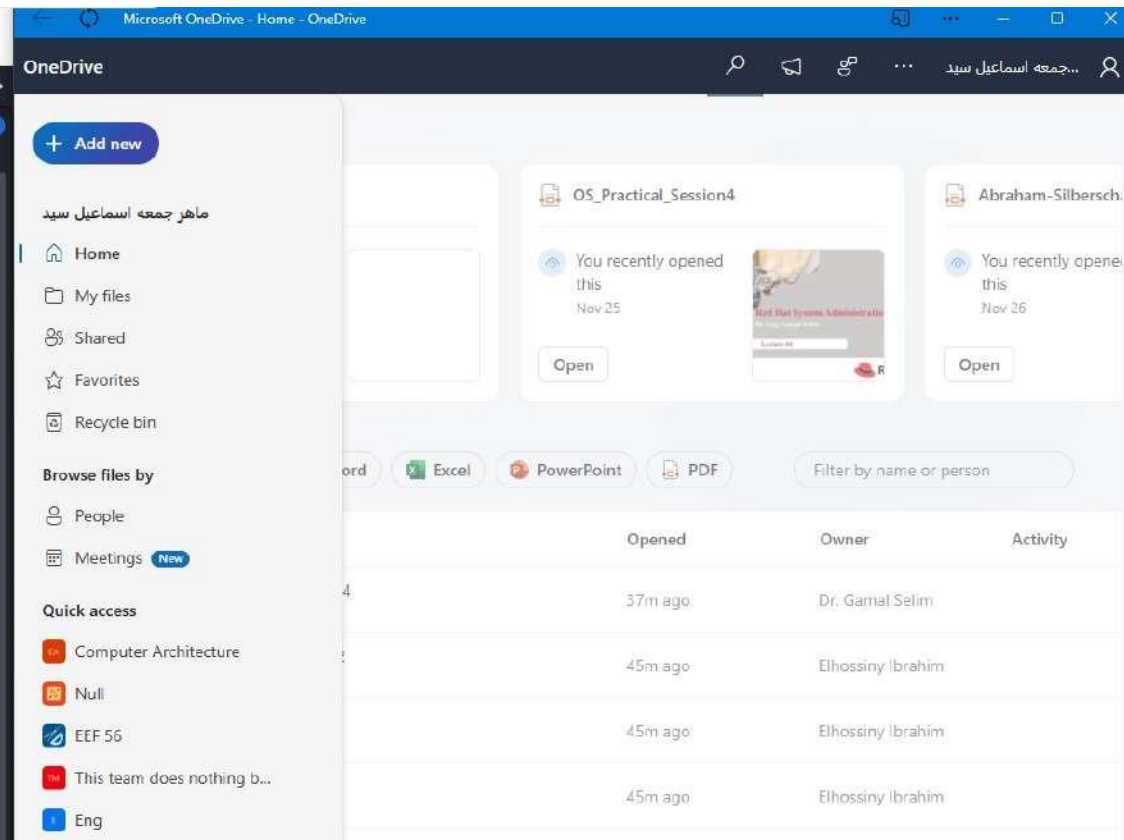

**Microsoft OneDrive:**

The OneDrive interface shows a sidebar with navigation options: Home, My files, Shared, Favorites, Recycle bin, Browse files by (People, Meetings), and Quick access. The main area displays a list of files and folders. A table of recent activity is visible:

Opened	Owner	Activity
34m ago	Dr. Gamal Selim	
42m ago	Elhossiny Ibrahim	
42m ago	Elhossiny Ibrahim	
42m ago	Elhossiny Ibrahim	
42m ago	Elhossiny Ibrahim	
42m ago	Elhossiny Ibrahim	
Dec 9	Dr. Gamal Selim	
Dec 6	ماهر جمعه اسماعيل سيد	You edited
Dec 3	Dr. Gamal Selim	
Nov 26	Dr. Gamal Selim	
Nov 24	Dr. Gamal Selim	

Here I used ping to see if the given site is up or not , and it's up by using ping command , we can also try nmap ww.google.com  
Then I terminate the process by Ctrl + C hotkey

```
Kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
m@kali: ~
File Actions Edit View Help
$ su n
Password:
(m@kali)-[~]
└─$ ping ww.google.com
PING ww3.l.google.com (172.217.171.238) 56(84) bytes of data:
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=1 ttl=118 time=48.2 ns
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=2 ttl=118 time=48.2 ns
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=3 ttl=118 time=48.1 ns
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=4 ttl=118 time=48.2 ns
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=5 ttl=118 time=48.8 ns
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=6 ttl=118 time=48.1 ns
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=7 ttl=118 time=47.8 ns
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=8 ttl=118 time=48.1 ns
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=9 ttl=118 time=47.9 ns
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=10 ttl=118 time=47.6 ms
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=11 ttl=118 time=48.5 ms
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=12 ttl=118 time=47.8 ms
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=13 ttl=118 time=47.9 ms
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=14 ttl=118 time=48.8 ms
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=15 ttl=118 time=47.9 ms
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=16 ttl=118 time=47.6 ms
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=17 ttl=118 time=47.5 ms
^C
```



Here I used nmap to gather some information about [www.google.com](http://www.google.com) I used the following options

-sV to know the version of port

-O to know the operating system

-sC to know more about ports that is open

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
m@kali: ~
File Actions Edit View Help
(m@kali): ~
$ sudo nmap -sV -O -sC www.google.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-16 08:04 EST
Nmap scan report for www.google.com (172.217.171.228)
Host is up (0.048s latency).
Other addresses for www.google.com (not scanned): 2a00:1450:4006:810::2004
rDNS record for 172.217.171.228: mrs09s07-in-f4.1e100.net
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (net-unreach)
PORT      STATE SERVICE VERSION
80/tcp    open  http      gws
_http-favicon: Google
_http-server-header: gws
_fingerprint-strings:
  GetRequest:
    HTTP/1.0 200 OK
    Date: Sat, 16 Dec 2023 13:05:02 GMT
    Expires: -1
    Cache-Control: private, max-age=0
    Content-Type: text/html; charset=ISO-8859-1
    Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-D0LF6G282-3eFak178aMmA' 'strict-dynami
c' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http://report-uri https://csp.withgoogle.com/csp/gws/other-hp
    P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
    Server: gws
    X-XSS-Protection: 0
    X-Frame-Options: SAMEORIGIN
    Set-Cookie: 1P_JAR=2023-12-16-13; expires=Mon, 15-Jan-2024 13:05:02 GMT; path=/; domain=.google.com; Secure
    Set-Cookie: AEC=Ackid1RSZCzr7oB9Hs5Xz-Xf13UeaDeZfDwt-uu3vDRouWmilucjkb9kNQ; expires=Thu, 13-Jun-2024 13:05:02 GMT; path=/; doma
in=.google.com; Secure; HttpOnly; SameSite=lax
    Set-Cookie: WID=511-QCW15ZhiST-Ur5wXHUVC89vTgQPI8AdCmKdAqC60i5yZwh2-Xc2JmT2ZQv7B9jocDUQJTfz
  HTTPOptions:
    HTTP/1.0 405 Method Not Allowed
    Allow: GET, HEAD
    Date: Sat, 16 Dec 2023 13:05:02 GMT
    Content-Type: text/html; charset=UTF-8
    Server: gws
    Content-Length: 1592
    X-XSS-Protection: 0
    X-Frame-Options: SAMEORIGIN
    <!DOCTYPE html>
    <html lang=en>
    <meta charset=utf-8>
    <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
    <title>Error 405 (Method Not Allowed)!!1</title>
    <style>
      *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto
0;max-width:390px;min-height:180px;padding:30px 0 15px}> > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no
-repeat;padding-right:205px}{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}media screen and
(max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#l
http-robots.txt: 225 disallowed entries (15 shown)
/search/sdch/groups/index.html? /? /?hl=nb
/?hl=nb&gws_rd=ssl/imgres/u/ /preferences/setprefs/default/m? /n/ /wnl?
_http-title: Google
443/tcp  open  ssl/https gws
_http-server-header: gws
ssl-cert: Subject: commonName=www.google.com
Subject Alternative Name: DNS:www.google.com
```

Microsoft OneDrive - Home - OneDrive

OneDrive

+

Add new

ماهر جمعه اسماعيل سيد

Home

My files

Shared

Favorites

Recycle bin

Browse files by

People

Meetings New

Quick access

Computer Architecture

Null

EEF 56

This team does nothing b...

Eng

Microprocessor & Interfac...

سورة إعدادي - 2020/2021

اضرات (رياضيات هندسية ٤)

More places...

Storage

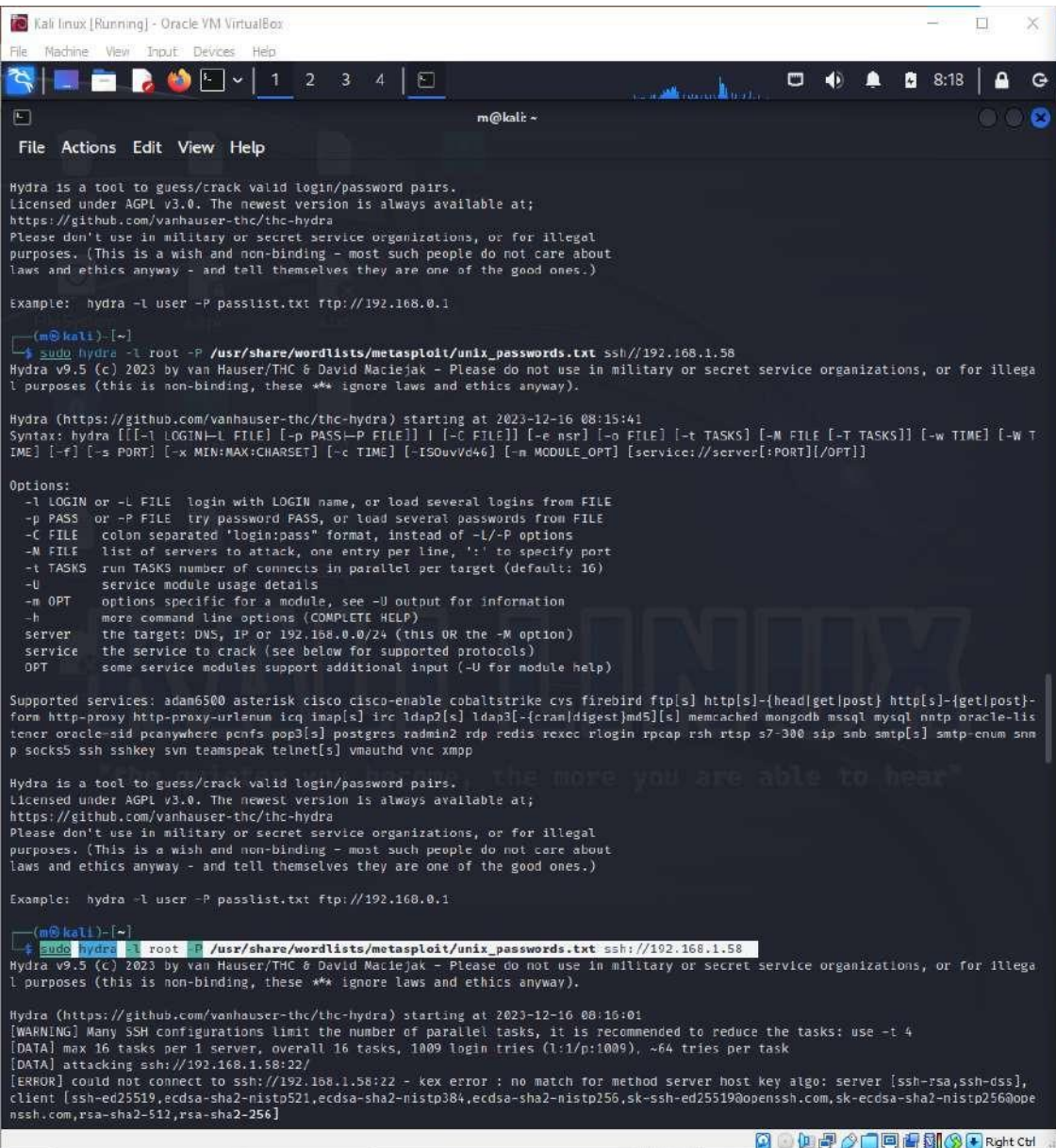
< 0.1 GB used of 5 TB (1%)

Opened	Owner	Activity
45m ago	Dr. Gamal Selim	
55m ago	Elhossiny Ibrahim	
55m ago	Elhossiny Ibrahim	
55m ago	Elhossiny Ibrahim	
55m ago	Elhossiny Ibrahim	
Dec 9	Dr. Gamal Selim	
Dec 6	ماهر جمعه اسماعيل سيد	You edited
Dec 3	Dr. Gamal Selim	
Nov 26	Dr. Gamal Selim	



Here we are trying to hack a metasploitable server by using hydra which is strong tool for trying username and passwords

I tried user "root" and list of password which is built-in called unix\_passwords to ssh://192.168.1.58:22 which is the ip of the server  
-l which L in lowercase means it will take the next argument as the user name will be trying with , and -P which is UpperCase used to pass a whole list with password to try it with the previous user name.



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

m@kali: ~
File Actions Edit View Help

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at:
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example: hydra -l user -P passlist.txt ftp://192.168.0.1

(m@kali):~$
$ sudo hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt ssh://192.168.1.58
Hydra v9.5 (c) 2023 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 2023-12-16 08:15:41
Syntax: hydra [[-l LOGIN|-L FILE] [-p PASS|-P FILE]] [-c C FILE] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W T
IME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISouVd46] [-m MODULE_OPT] [service://server[:PORT][:/OPT]]

Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-c FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-m OPT options specific for a module, see -U output for information
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)

Supported services: adan6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-
form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cran|digest}|md5][s] memcached mongodb mssql mysql nntp oracle-lis
tenser oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcac rsh rtsp s7-300 sip snb smtp[s] smtp-cnum snn
p socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpmp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at:
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example: hydra -l user -P passlist.txt ftp://192.168.0.1

(m@kali):~$
$ sudo hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt ssh://192.168.1.58
Hydra v9.5 (c) 2023 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 2023-12-16 08:16:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1809 login tries (1:1/p:1009), ~64 tries per task
[DATA] attacking ssh://192.168.1.58:22/
[ERROR] could not connect to ssh://192.168.1.58:22 - kex error : no match for method server host key algo: server [ssh-rsa,ssh-dss],
client [ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@ope
nssh.com,rsa-sha2-512,rsa-sha2-256]
```

