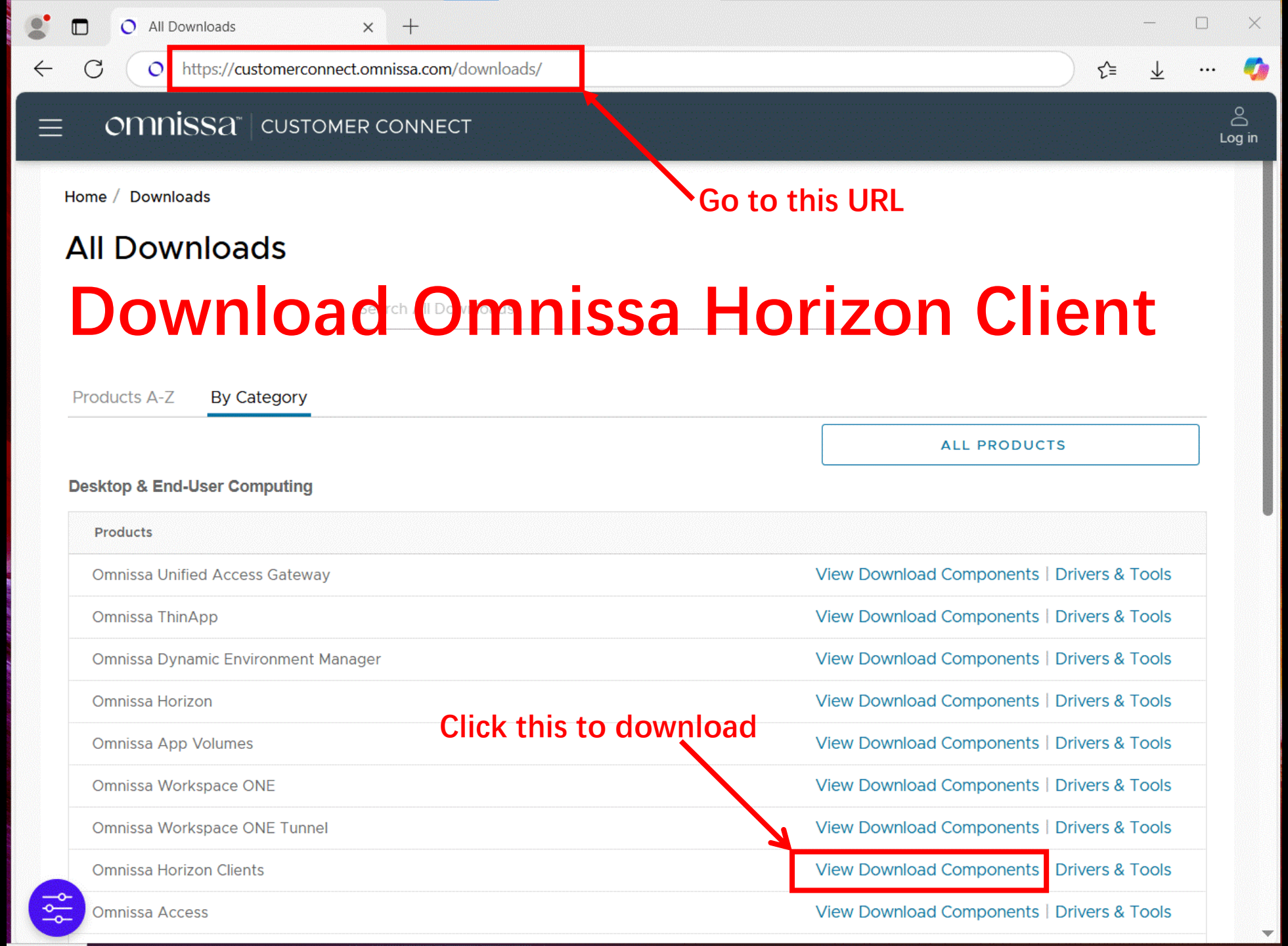
Lab01 Getting Started

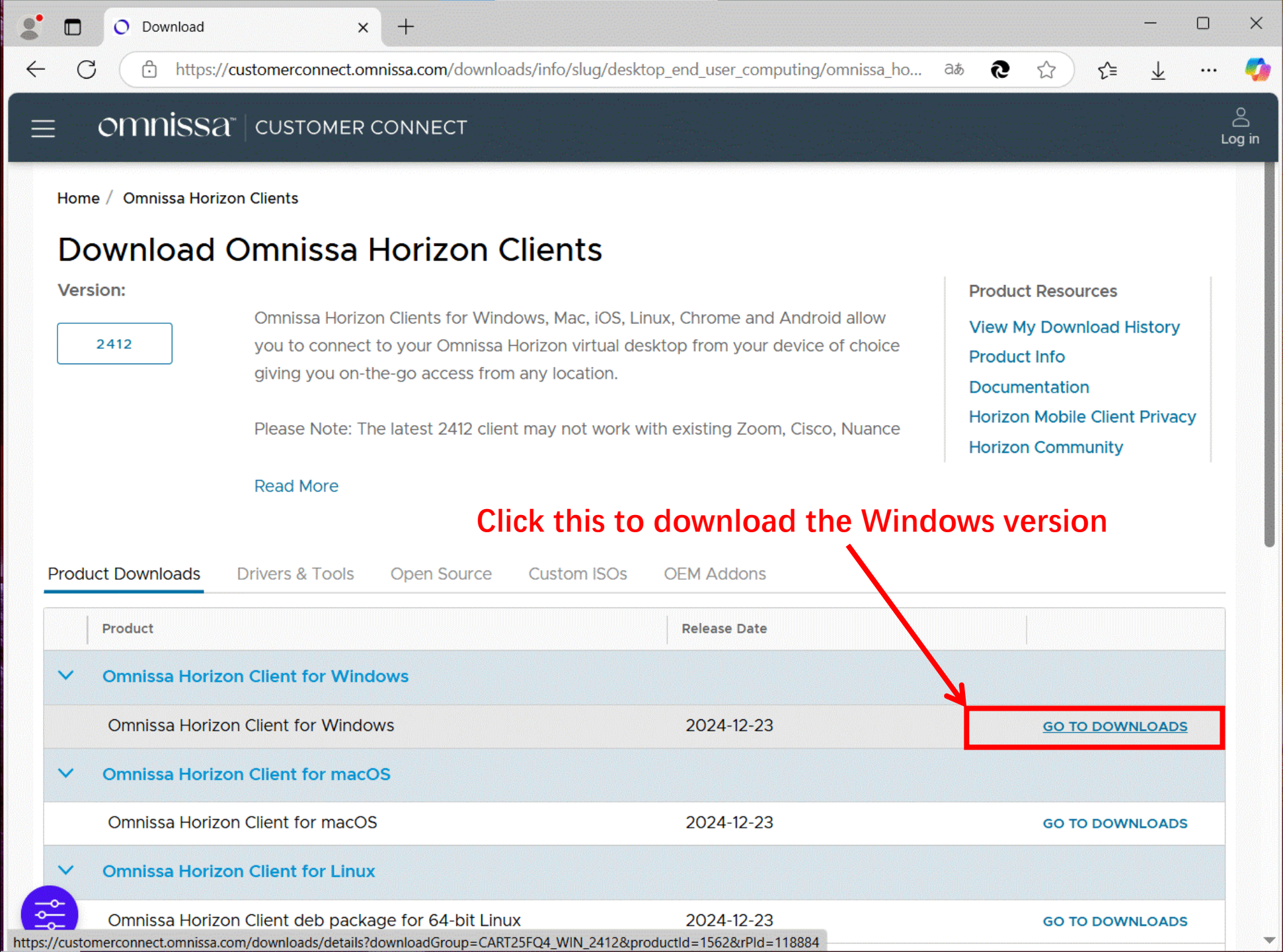
Prepared By Wooi Ping Cheah

Reference: COMP3052.SEC GETTING STARTED WITH KALI by Mike Pound

Accessing UNNC's Virtual Desktop Infrastructure

- In this lab session, you will do your work using the software pre-installed and pre-configured on the UNNC's Virtual Desktop Infrastructure (VDI).
- You will mainly use the software called Oracle VM VirtualBox pre-installed and pre-configured on the UNNC's VDI.
- Oracle VM VirtualBox is a virtual machine that allows multiple operating systems, such as Kali-Linux and Ubuntu to run on a Windows workstation.
- Most of our lab exercises and assignments for this module will be on Kali-Linux or Ubuntu.
- Firstly, we want you to install and configure a software called Omnissa Horizon Client to your local device (pc, laptop, etc..) so that it can be used to access the UNNC's VDI remotely over a network.


All Downloads
https://customerconnect.omnissa.com/downloads/
omnissa | CUSTOMER CONNECT
Log in
Go to this URL
Home / Downloads
All Downloads
Download Omnissa Horizon Client
Products A-Z
By Category
ALL PRODUCTS
Desktop & End-User Computing
Products
Omnissa Unified Access Gateway
Omnissa ThinApp
Omnissa Dynamic Environment Manager
Omnissa Horizon
Omnissa App Volumes
Omnissa Workspace ONE
Omnissa Workspace ONE Tunnel
Omnissa Horizon Clients
Omnissa Access
View Download Components | Drivers & Tools
Click this to download


Download
https://customerconnect.omnissa.com/downloads/info/slug/desktop_end_user_computing/omnissa_ho...
omnissa | CUSTOMER CONNECT
Log in
Home / Omnissa Horizon Clients
Download Omnissa Horizon Clients
Version:
2412
Omnissa Horizon Clients for Windows, Mac, iOS, Linux, Chrome and Android allow you to connect to your Omnissa Horizon virtual desktop from your device of choice giving you on-the-go access from any location.
Please Note: The latest 2412 client may not work with existing Zoom, Cisco, Nuance
Read More
Product Resources
View My Download History
Product Info
Documentation
Horizon Mobile Client Privacy
Horizon Community
Click this to download the Windows version
Product Downloads
Drivers & Tools
Open Source
Custom ISOs
OEM Addons
Product
Release Date
Omnissa Horizon Client for Windows
Omnissa Horizon Client for Windows
2024-12-23
GO TO DOWNLOADS
Omnissa Horizon Client for macOS
Omnissa Horizon Client for macOS
2024-12-23
GO TO DOWNLOADS
Omnissa Horizon Client for Linux
Omnissa Horizon Client deb package for 64-bit Linux
2024-12-23
GO TO DOWNLOADS
https://customerconnect.omnissa.com/downloads/details?downloadGroup=CART25FQ4_WIN_2412&productId=1562&rPId=118884

Download

https://customerconnect.omnissa.com/downloads/details?downloadGroup=CART25FQ4_WIN_2412&pr...

omnissa | CUSTOMER CONNECT

Log in

Home / Omnissa Horizon Client for Windows

Download Product

Version	2412
Documentation	Release Notes
Release Date	2024-12-23
Type	Product Binaries

Product Resources

- View My Download History
- Product Info
- Documentation
- Horizon Mobile Client Privacy
- Horizon Community

Click this to start downloading

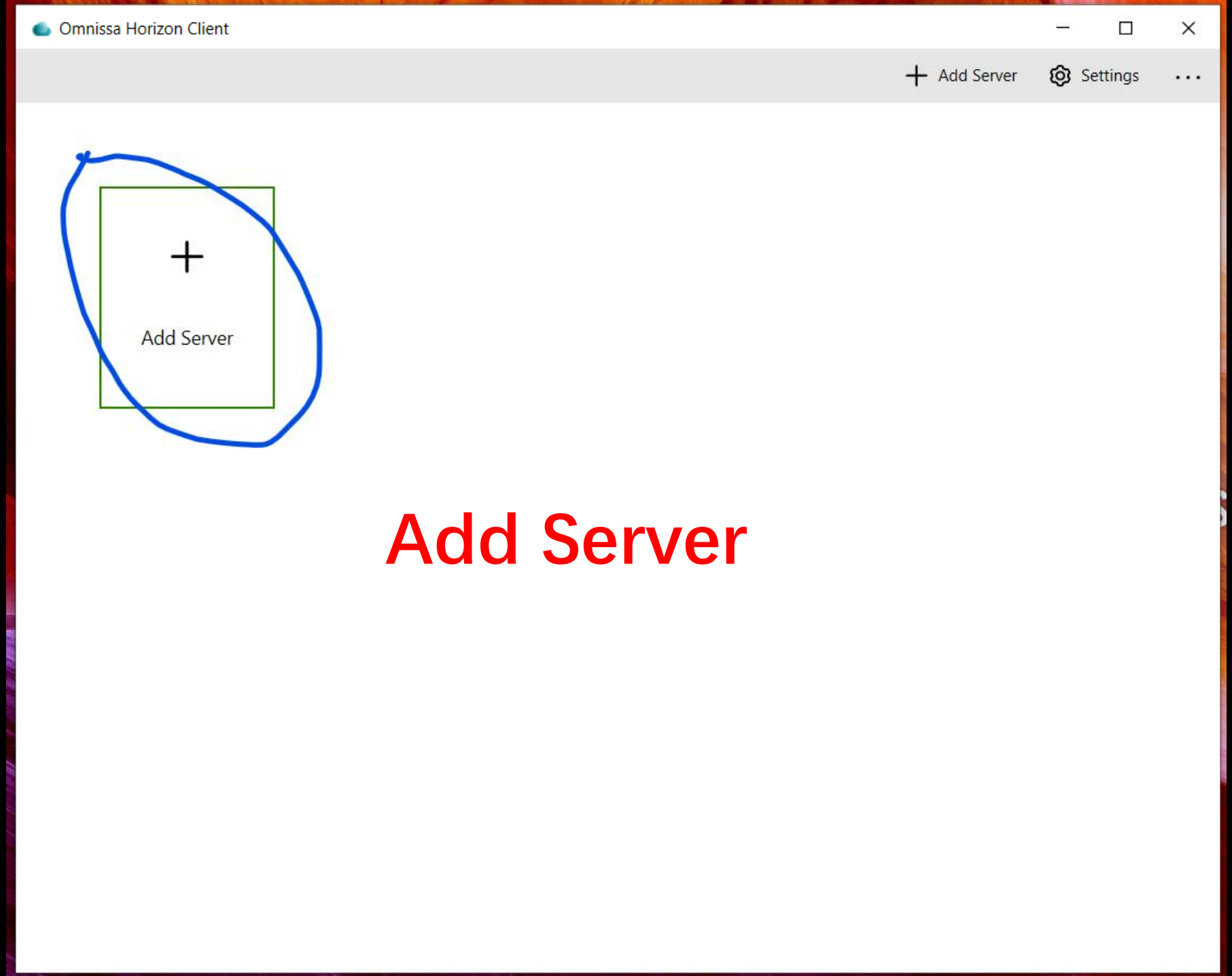
Product Downloads | Drivers & Tools | Open Source | Custom ISOs | OEM Addons

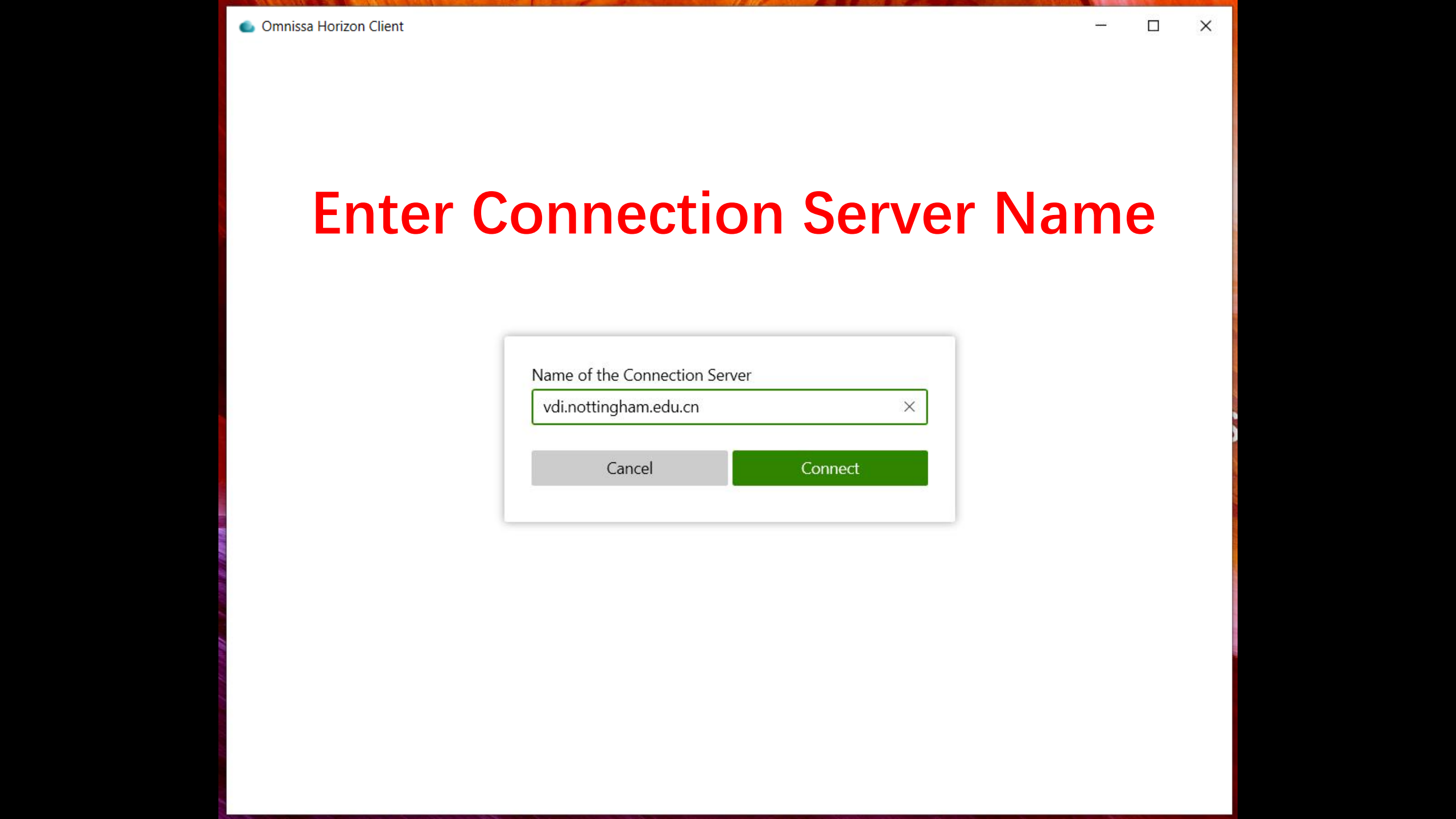
File	Information
Omnissa Horizon Windows Client File size: 292.97 MB File type: exe Read More	DOWNLOAD NOW

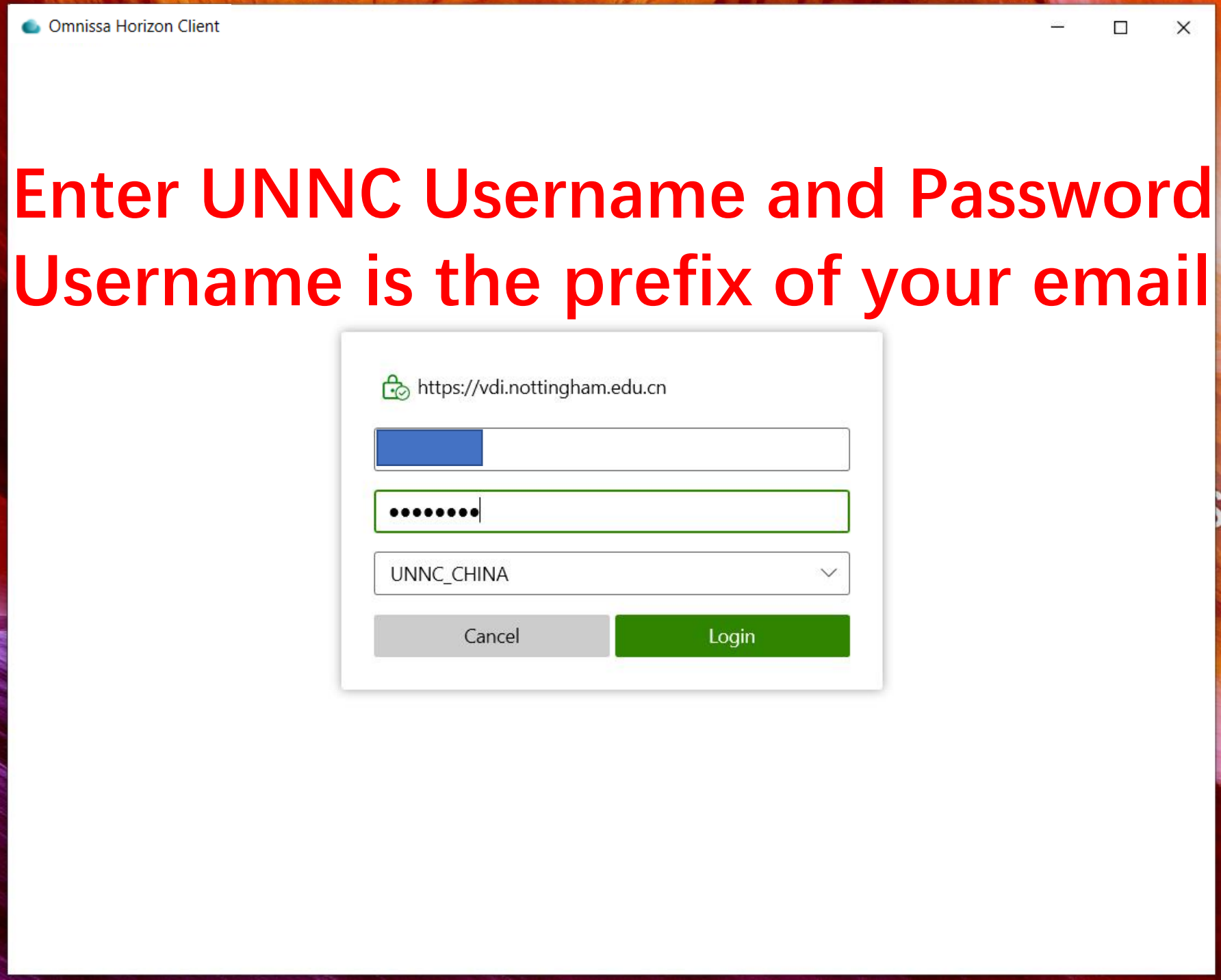
https://download3.omnissa.com/software/CART25FQ4_WIN_2412/Omnissa-Horizon-Client-2412-8.14.0-12437220870.exe

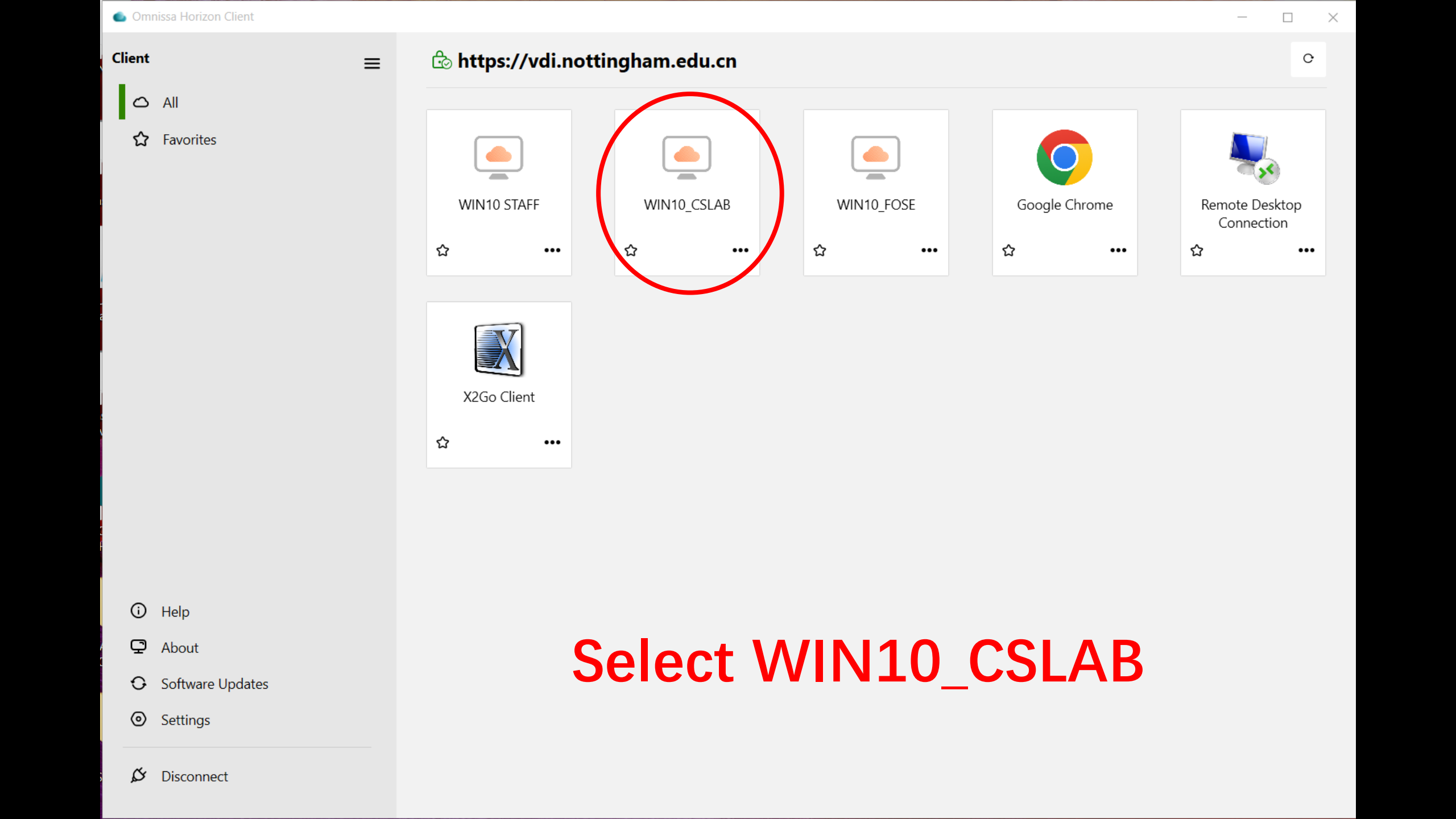

This PC
Omnissa-Horizon-Client-2412-8.14.0-12437220870.exe
Recycle Bin
User
Control Pane
Outlook
Launch Omnissa Horizon Client Installer
Installation May Take Some Time

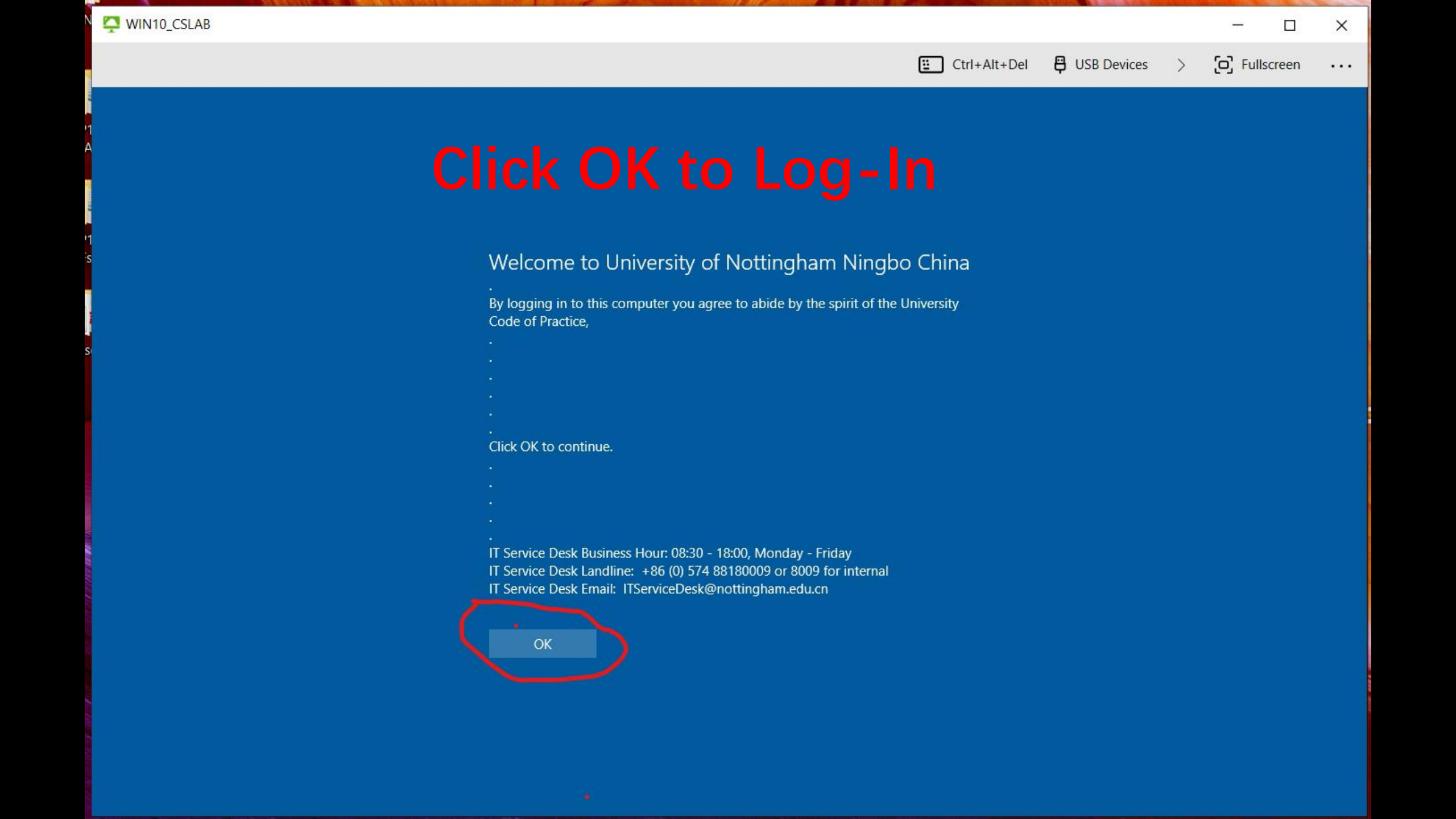

This PC
Omnissa-Ho...
Recycle Bin
Omnissa Horizon Client
User
Control Pane
Outlook
After the Installation Completed
Launch Omnissa Horizon Client

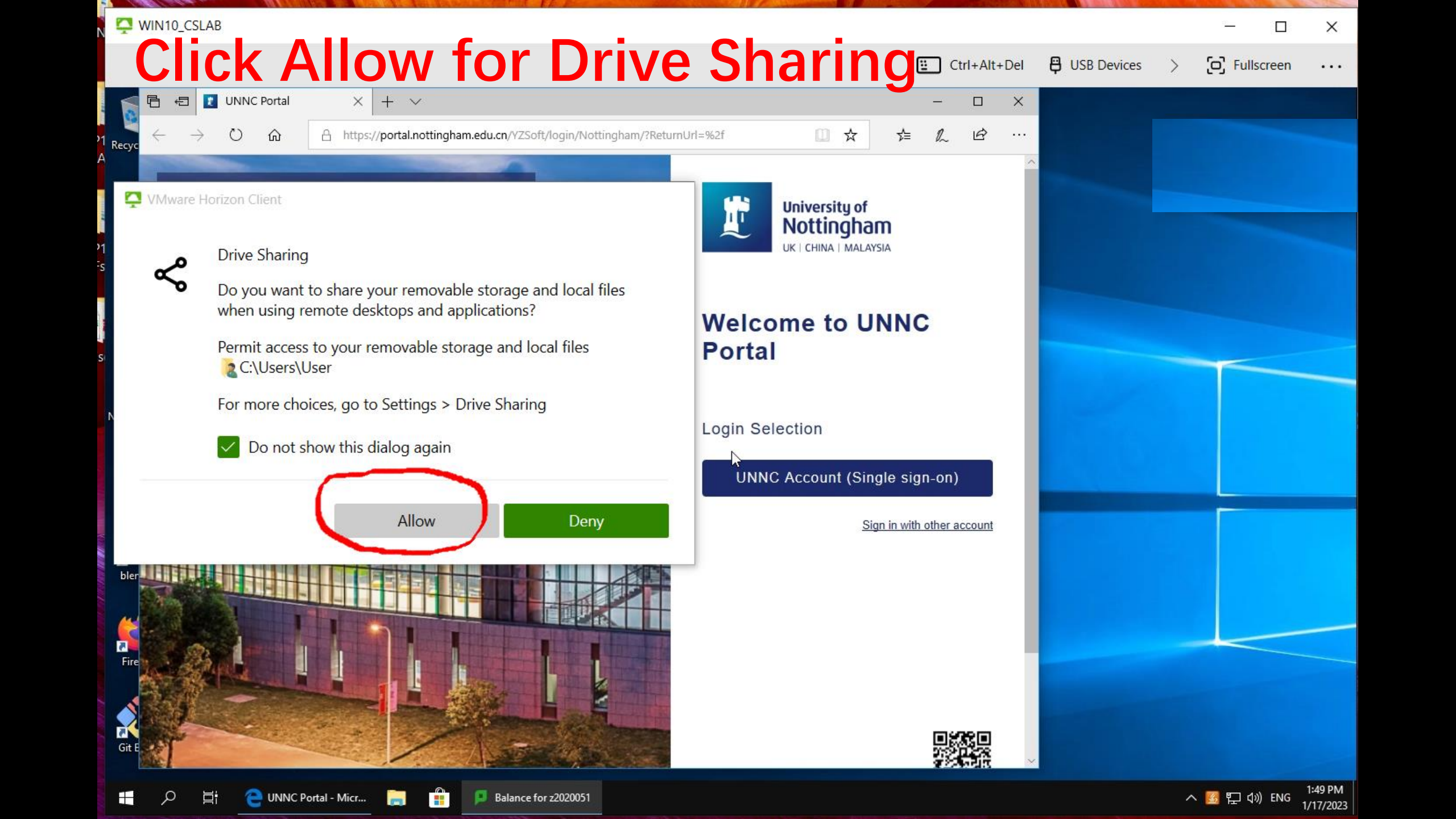

Omnissa Horizon Client
Add Server
Settings
Add Server
Add Server

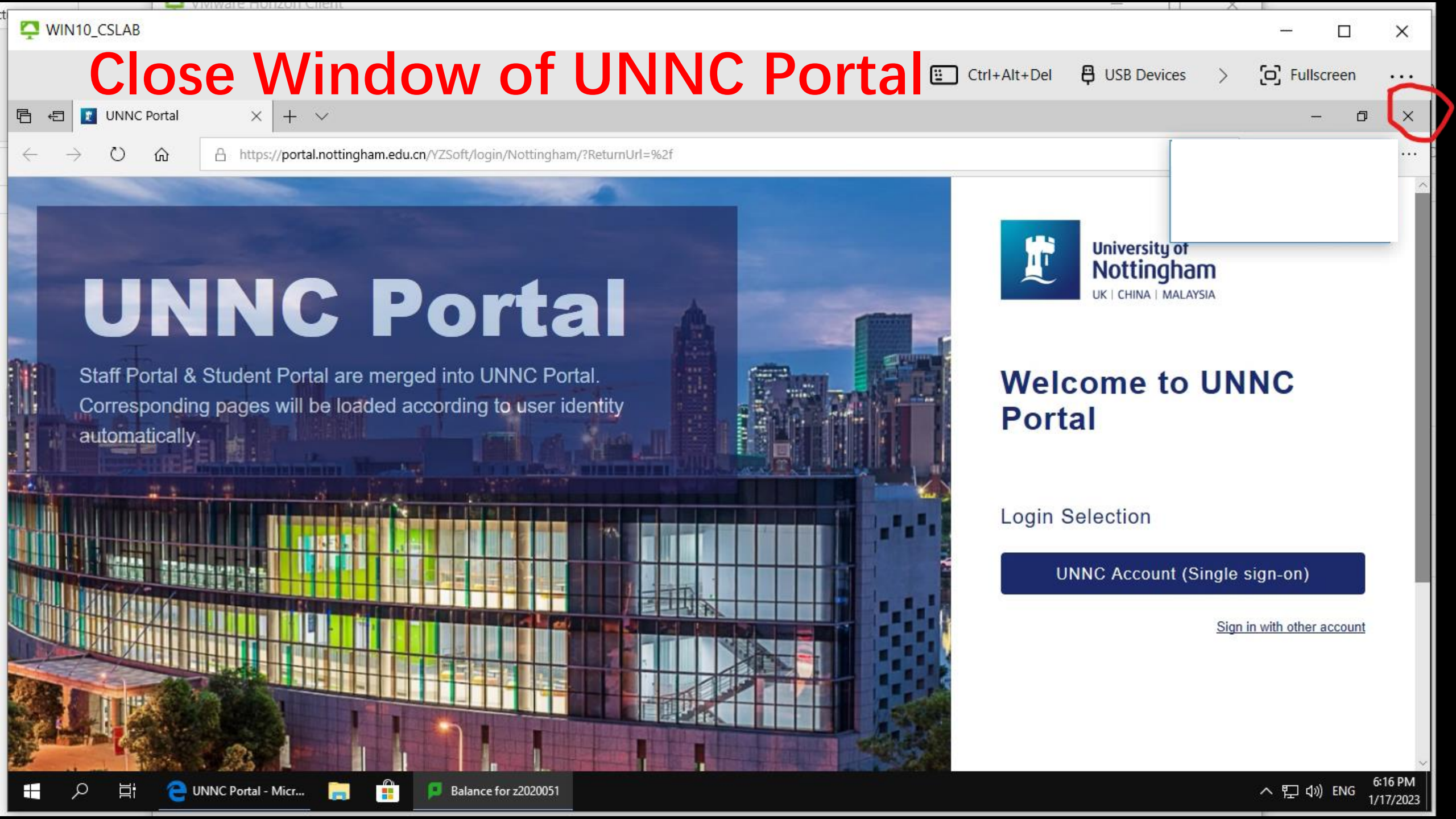

Omnissa Horizon Client
Enter Connection Server Name
Name of the Connection Server
vdi.nottingham.edu.cn
Cancel
Connect


Omnissa Horizon Client
Enter UNNC Username and Password
Username is the prefix of your email
https://vdi.nottingham.edu.cn
UNNC_CHINA
Cancel
Login


Omnissa Horizon Client
Client
All
Favorites
https://vdi.nottingham.edu.cn
WIN10 STAFF
WIN10_CSLAB
WIN10_FOSE
Google Chrome
Remote Desktop Connection
X2Go Client
Help
About
Software Updates
Settings
Disconnect
Select WIN10_CSLAB

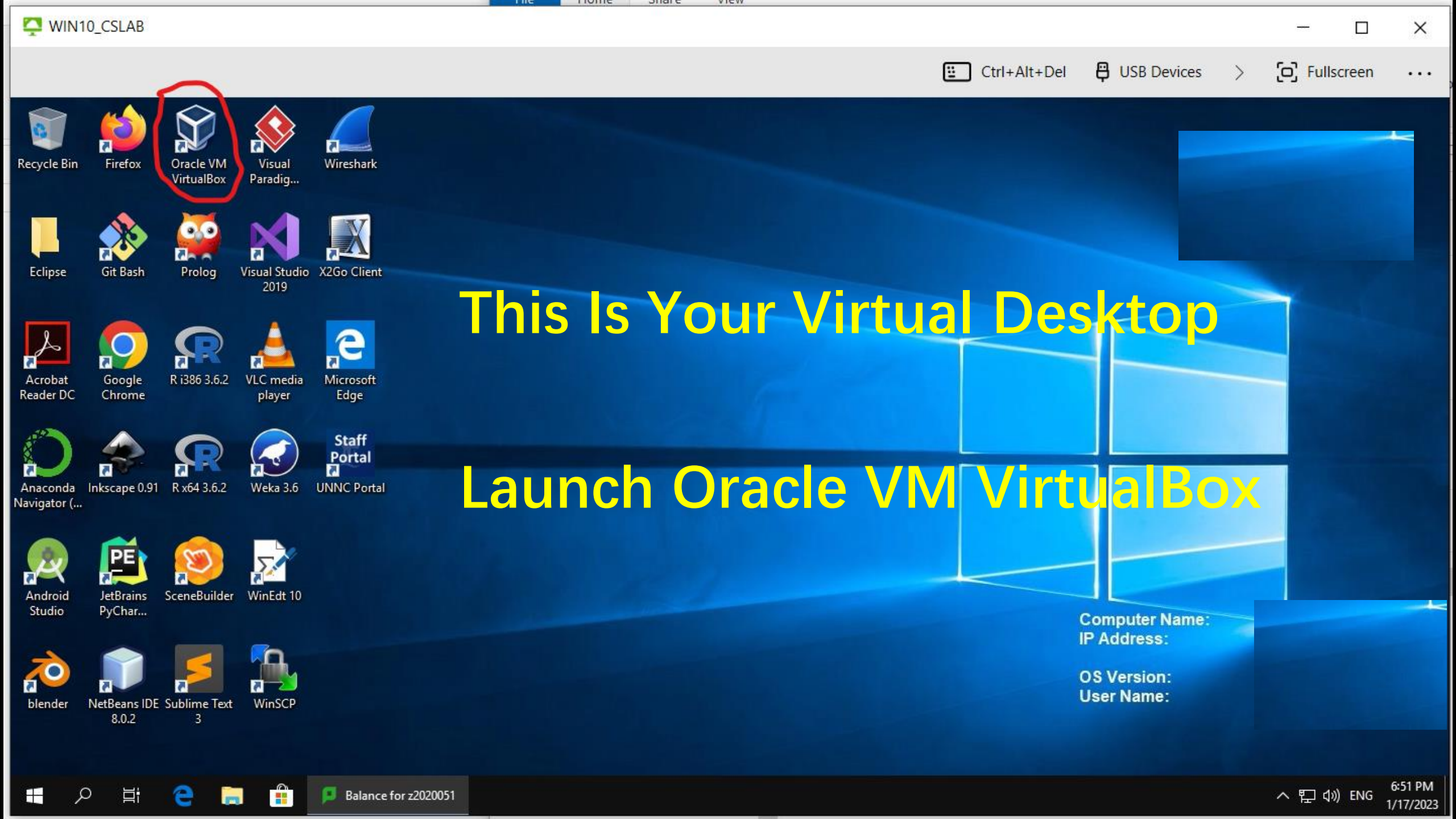

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Click OK to Log-In
Welcome to University of Nottingham Ningbo China
By logging in to this computer you agree to abide by the spirit of the University Code of Practice,
Click OK to continue.
IT Service Desk Business Hour: 08:30 - 18:00, Monday - Friday
IT Service Desk Landline: +86 (0) 574 88180009 or 8009 for internal
IT Service Desk Email: ITServiceDesk@nottingham.edu.cn
OK

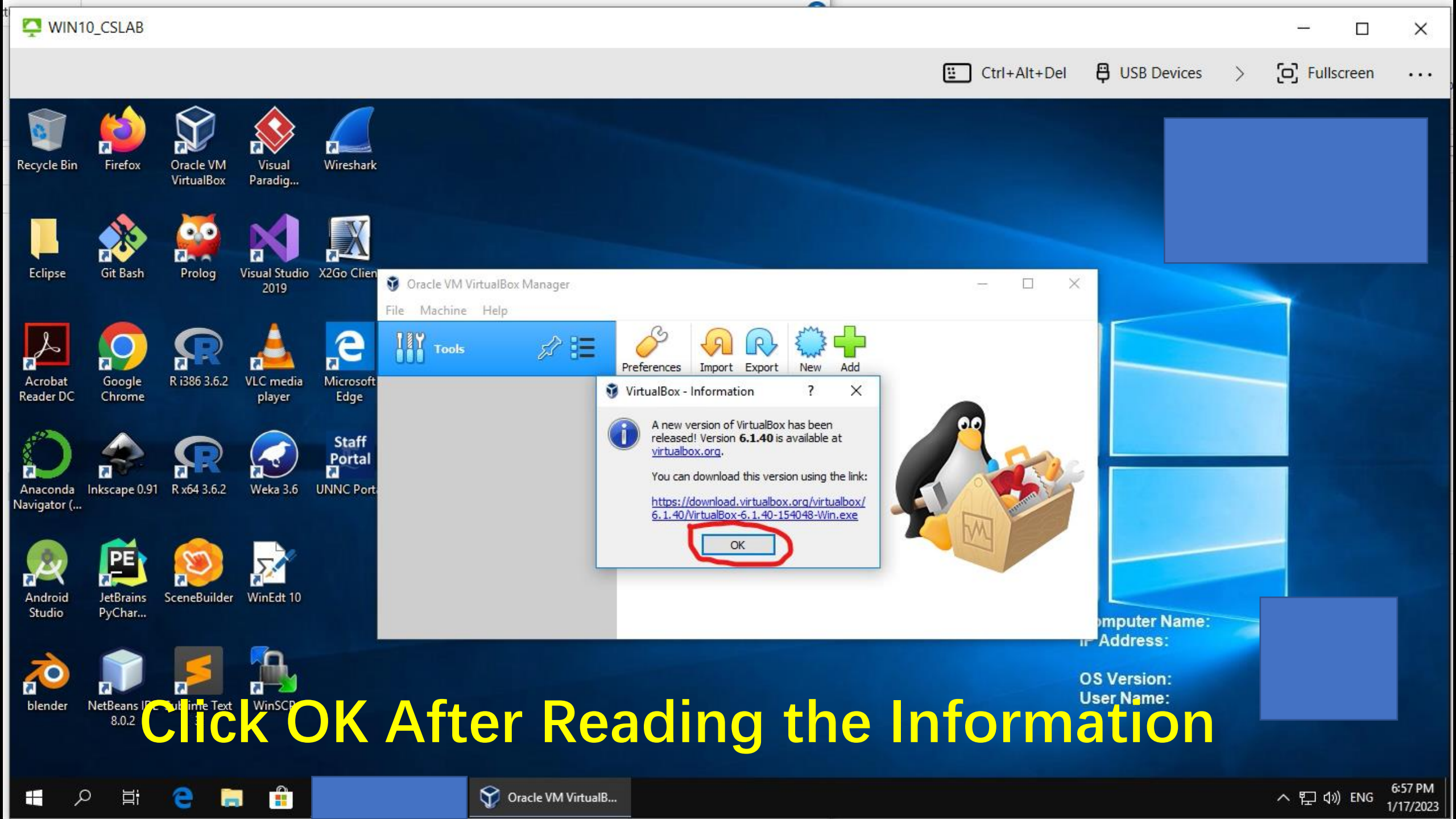

Click Allow for Drive Sharing
WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
UNNC Portal
https://portal.nottingham.edu.cn/YZSoft/login/Nottingham/?ReturnUrl=%2f
VMware Horizon Client
Drive Sharing
Do you want to share your removable storage and local files when using remote desktops and applications?
Permit access to your removable storage and local files
C:\Users\User
For more choices, go to Settings > Drive Sharing
Do not show this dialog again
Allow
Deny
University of Nottingham
UK | CHINA | MALAYSIA
Welcome to UNNC Portal
Login Selection
UNNC Account (Single sign-on)
Sign in with other account
UNNC Portal - Micr...
Balance for z2020051
ENG
1:49 PM
1/17/2023


WIN10_CSLAB
Close Window of UNNC Portal
Ctrl+Alt+Del
USB Devices
Fullscreen
UNNC Portal
https://portal.nottingham.edu.cn/YZSoft/login/Nottingham/?ReturnUrl=%2f
UNNC Portal
Staff Portal & Student Portal are merged into UNNC Portal.
Corresponding pages will be loaded according to user identity automatically.
University of Nottingham
UK | CHINA | MALAYSIA
Welcome to UNNC Portal
Login Selection
UNNC Account (Single sign-on)
Sign in with other account
UNNC Portal - Micr...
Balance for z2020051
ENG
6:16 PM
1/17/2023

Configuring Oracle VM VirtualBox

- You have successfully logged in to your UNNC virtual desktop. It looks and feels like a physical workstation, and many applications are readily available to you.
- You will experience your virtual desktop exactly the same way every time you log in, no matter which device you are logging into it from.
- You may not be able to save changes or permanently install applications on your virtual desktop.
- Your next task is to configure your VM VirtualBox by selecting the virtual machines (i.e., Kali-Linux and Ubuntu) and doing the necessary settings.
- You can quickly set up and run pre-configured virtual machines by importing an Open Virtual Appliance (OVA) file, without the hassle of manually configuring each component.
- An OVA file is a standardized package format that contains a virtual machine's disk image, configuration settings, and other necessary files. The OVA file you will import is called SEC2021VMs.


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Recycle Bin
Firefox
Oracle VM VirtualBox
Visual Paradig...
Wireshark
Eclipse
Git Bash
Prolog
Visual Studio 2019
X2Go Client
Acrobat Reader DC
Google Chrome
R i386 3.6.2
VLC media player
Microsoft Edge
Anaconda Navigator (...
Inkscape 0.91
R x64 3.6.2
Weka 3.6
Staff Portal
UNNC Portal
Android Studio
JetBrains PyChar...
SceneBuilder
WinEdt 10
blender
NetBeans IDE 8.0.2
Sublime Text 3
WinSCP
This Is Your Virtual Desktop
Launch Oracle VM VirtualBox
Computer Name:
IP Address:
OS Version:
User Name:
Balance for z2020051
ENG
6:51 PM
1/17/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Recycle Bin
Firefox
Oracle VM VirtualBox
Visual Paradig...
Wireshark
Eclipse
Git Bash
Prolog
Visual Studio 2019
X2Go Clien
Acrobat Reader DC
Google Chrome
R i386 3.6.2
VLC media player
Microsoft Edge
Anaconda Navigator (...
Inkscape 0.91
R x64 3.6.2
Weka 3.6
Staff Portal
UNNC Port
Android Studio
JetBrains PyChar...
SceneBuilder
WinEdt 10
blender
NetBeans IDE 8.0.2
Sublime Text
WinSCP
Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Preferences
Import
Export
New
Add
VirtualBox - Information
A new version of VirtualBox has been released! Version 6.1.40 is available at virtualbox.org.
You can download this version using the link:
https://download.virtualbox.org/virtualbox/6.1.40/VirtualBox-6.1.40-154048-Win.exe
OK
Computer Name:
IP Address:
OS Version:
User Name:
Click OK After Reading the Information
Oracle VM VirtualB...
ENG
6:57 PM
1/17/2023

Oracle VM VirtualBox Manager

File Machine Help

Tools

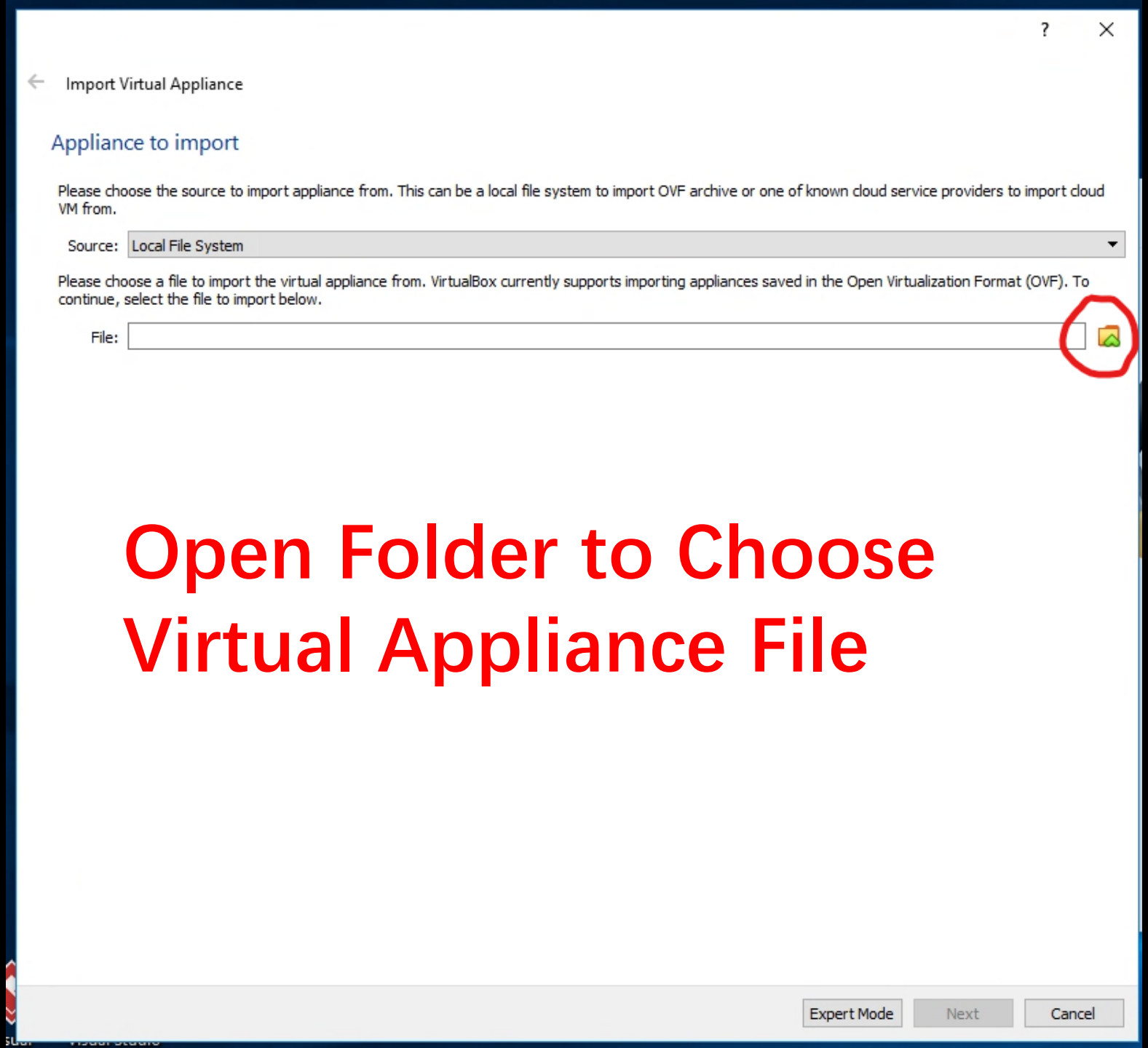
Preferences Import Export New Add

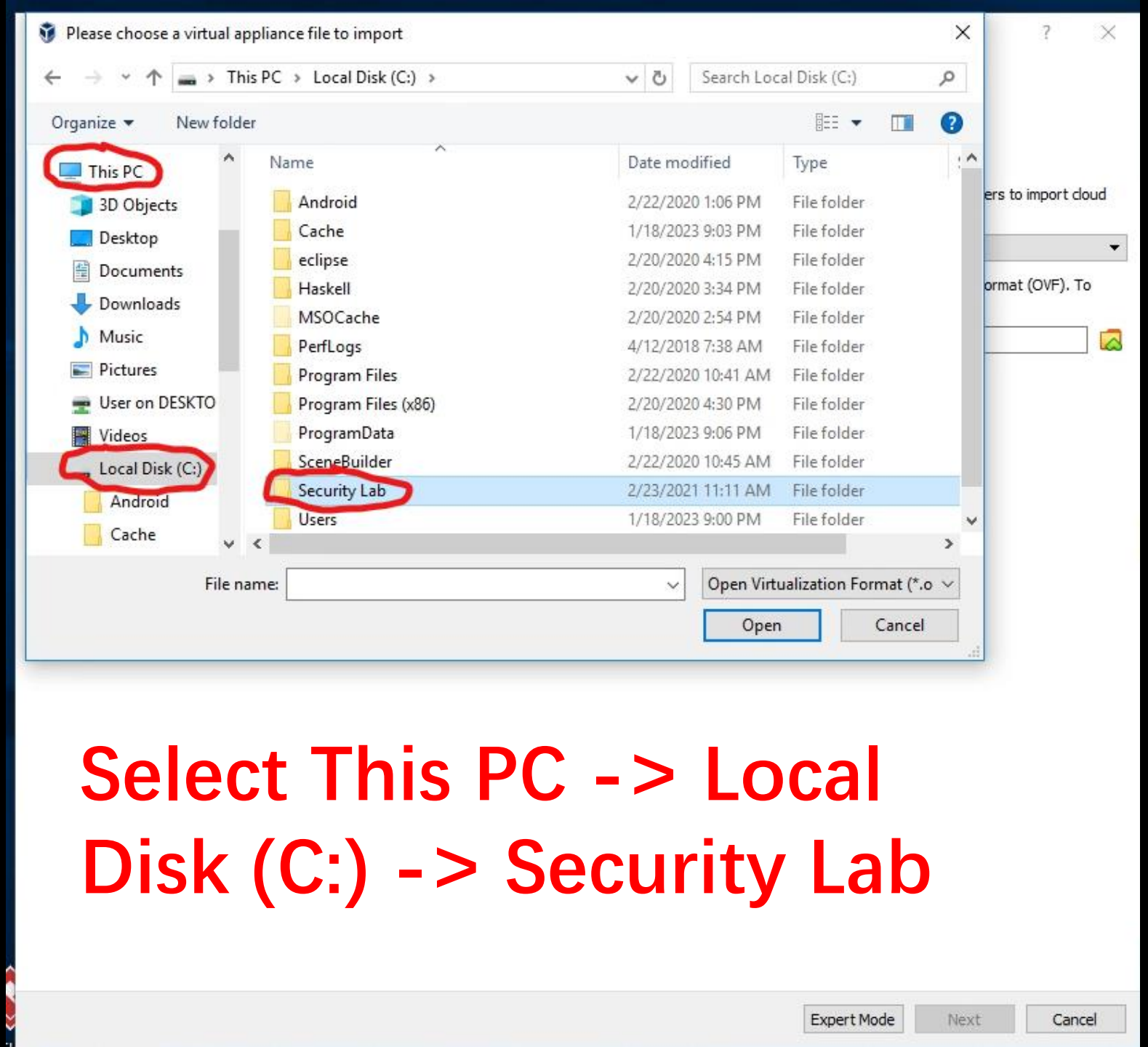
Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

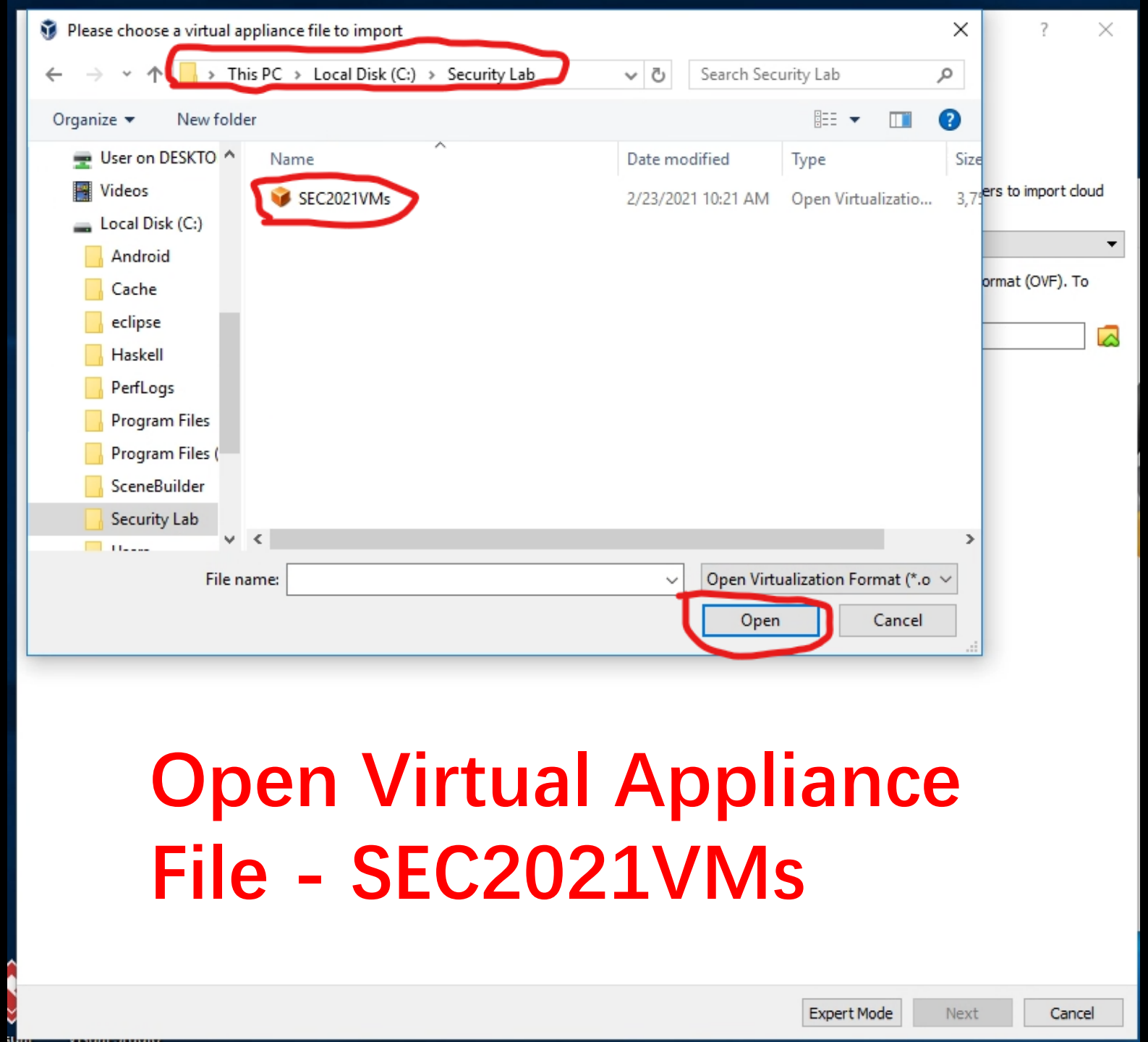
You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Import Virtual Appliances

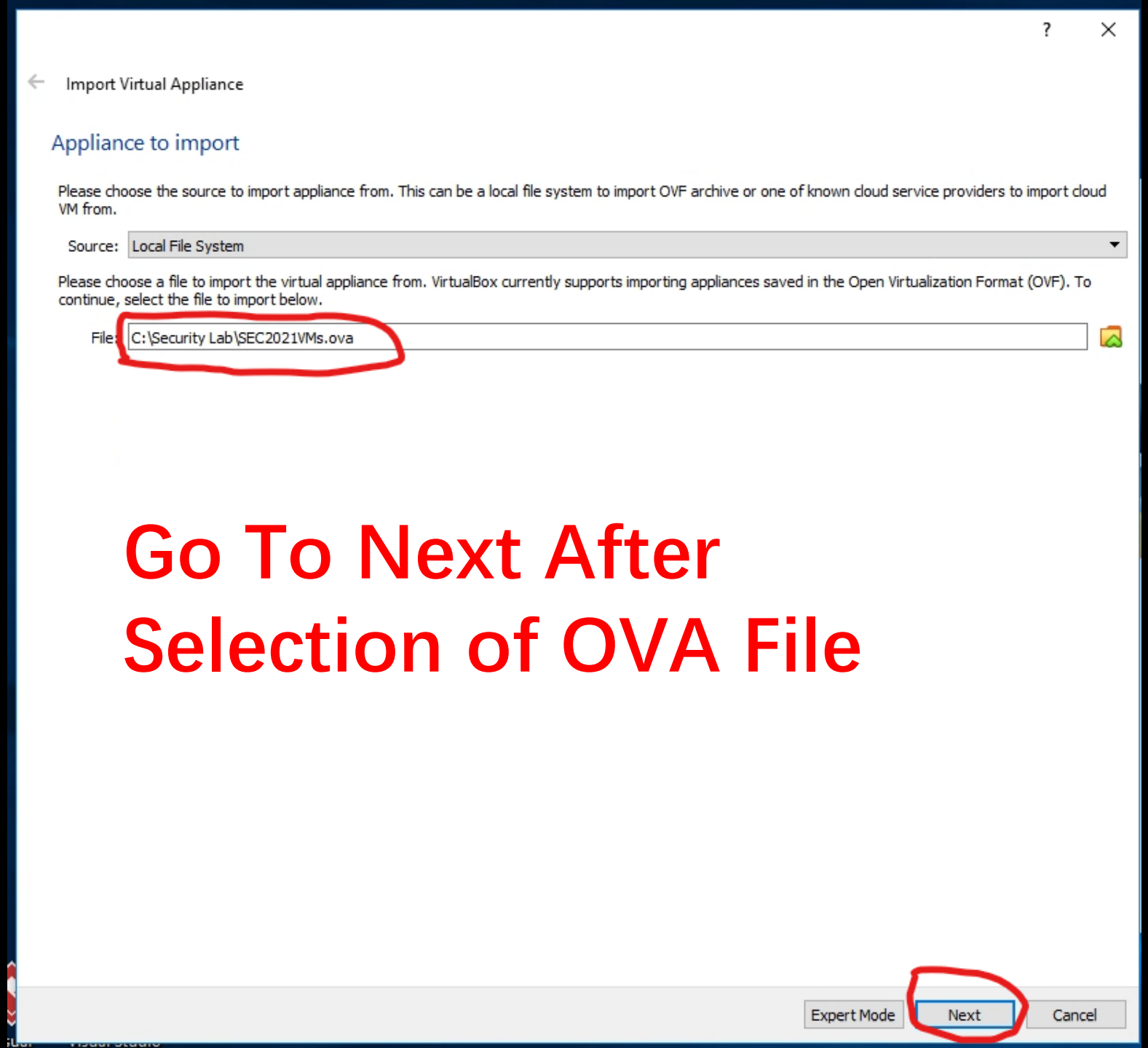

Import Virtual Appliance
Appliance to import
Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.
Source:
Local File System
Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.
File:
Open Folder to Choose Virtual Appliance File
Expert Mode
Next
Cancel

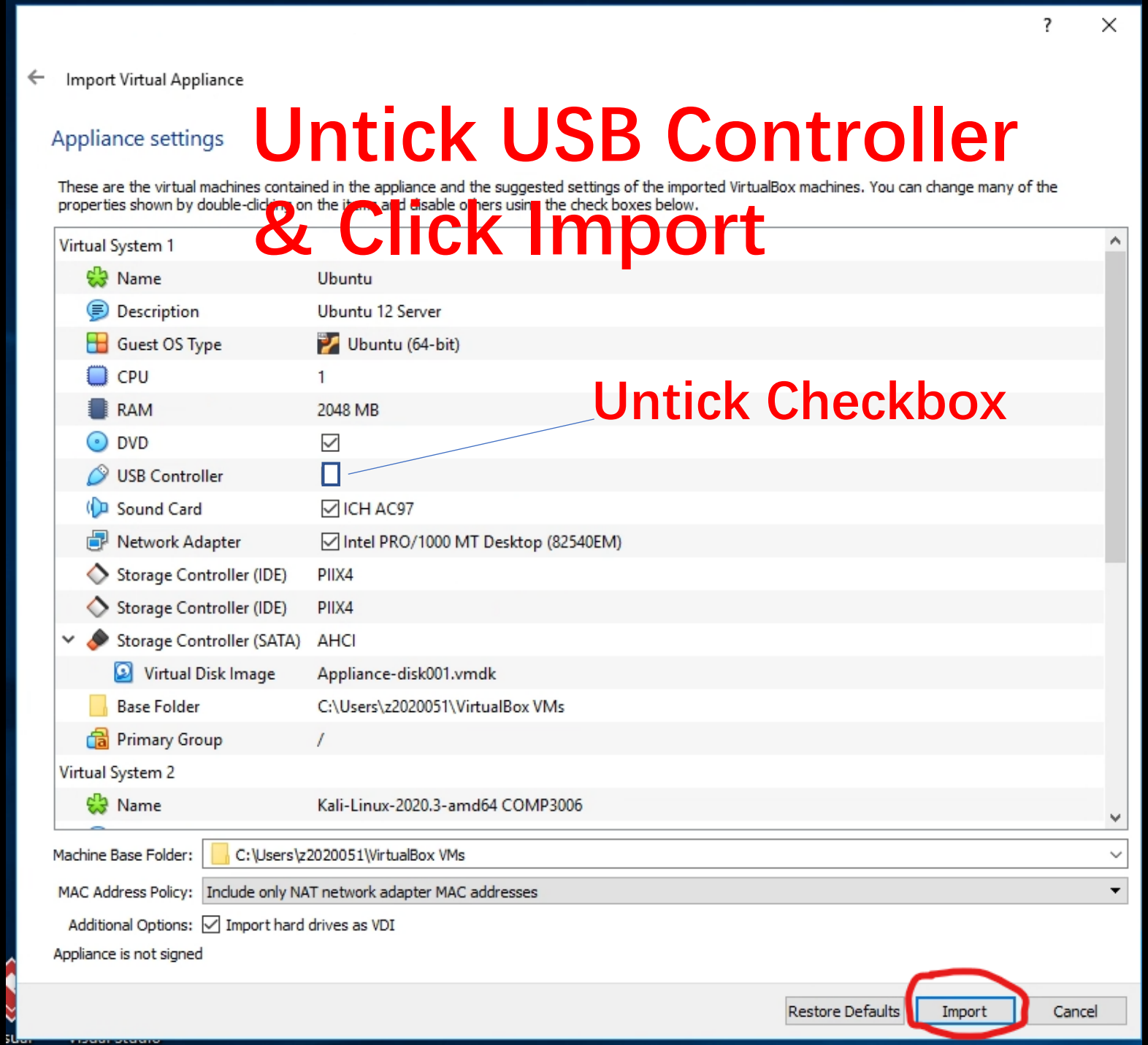


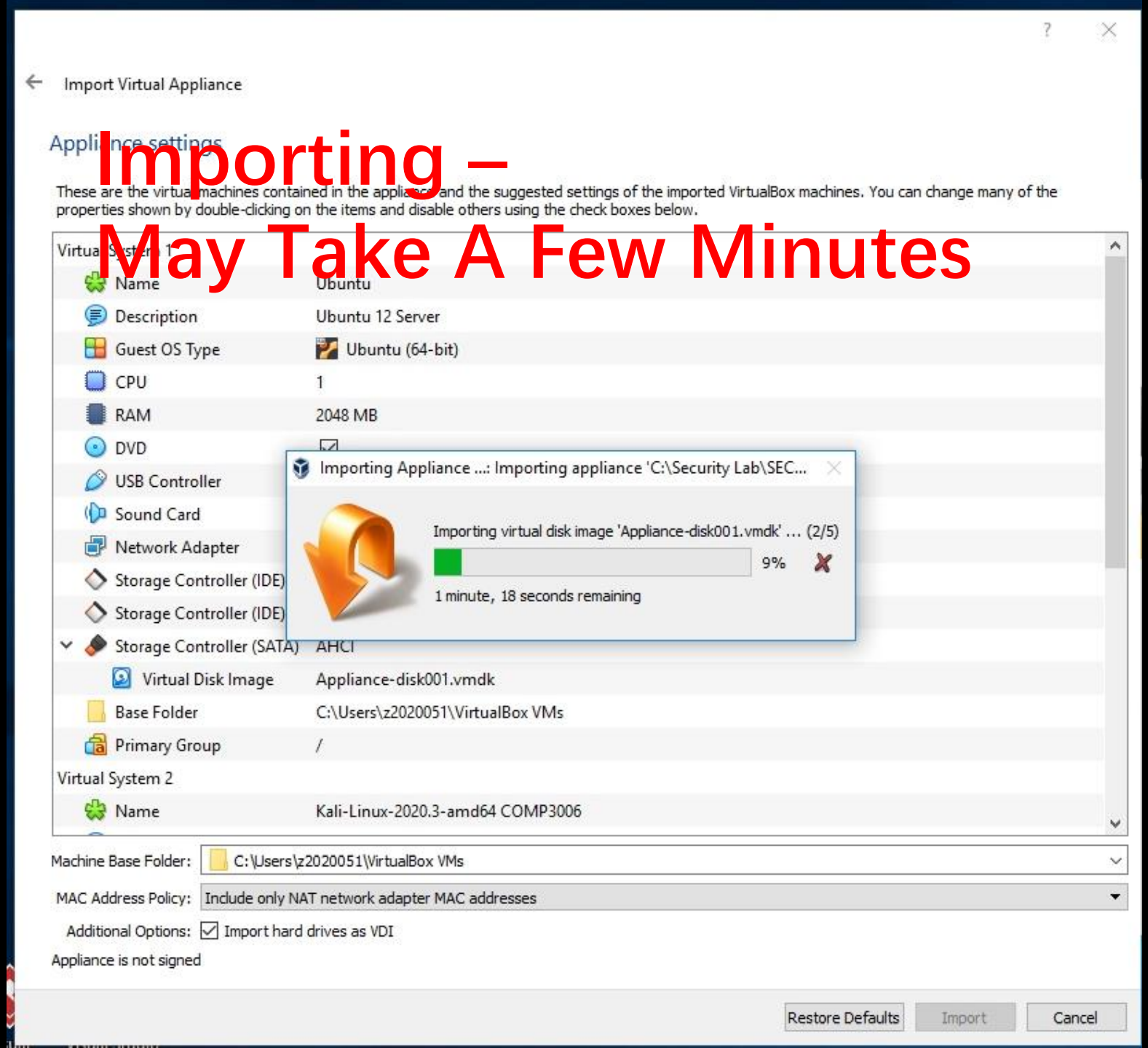
Select This PC -> Local Disk (C:) -> Security Lab

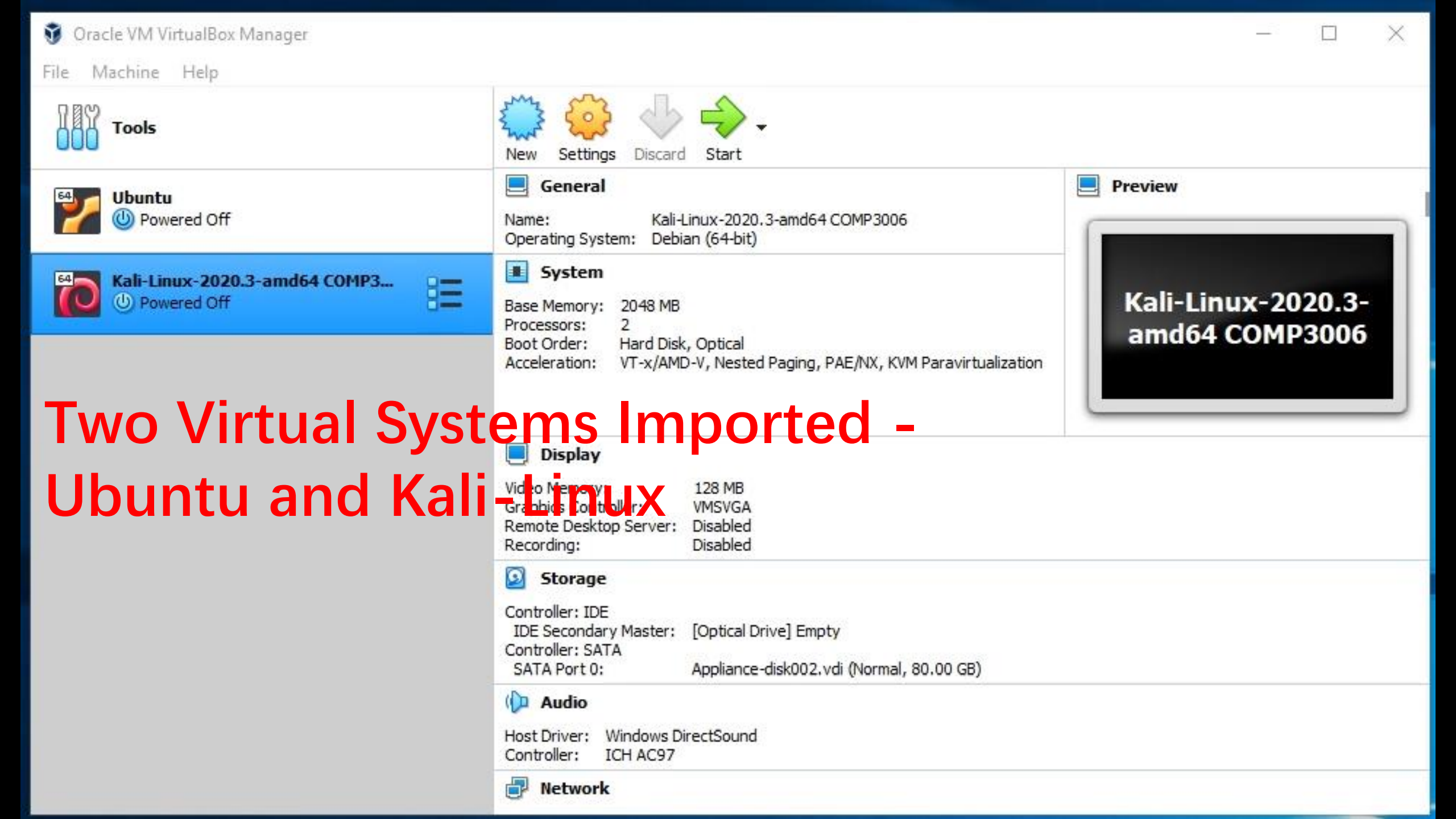


Open Virtual Appliance File - SEC2021VMs


Import Virtual Appliance
Appliance to import
Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.
Source:
Local File System
Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.
File:
C:\Security Lab\SEC2021VMs.ova
Go To Next After Selection of OVA File
Expert Mode
Next
Cancel

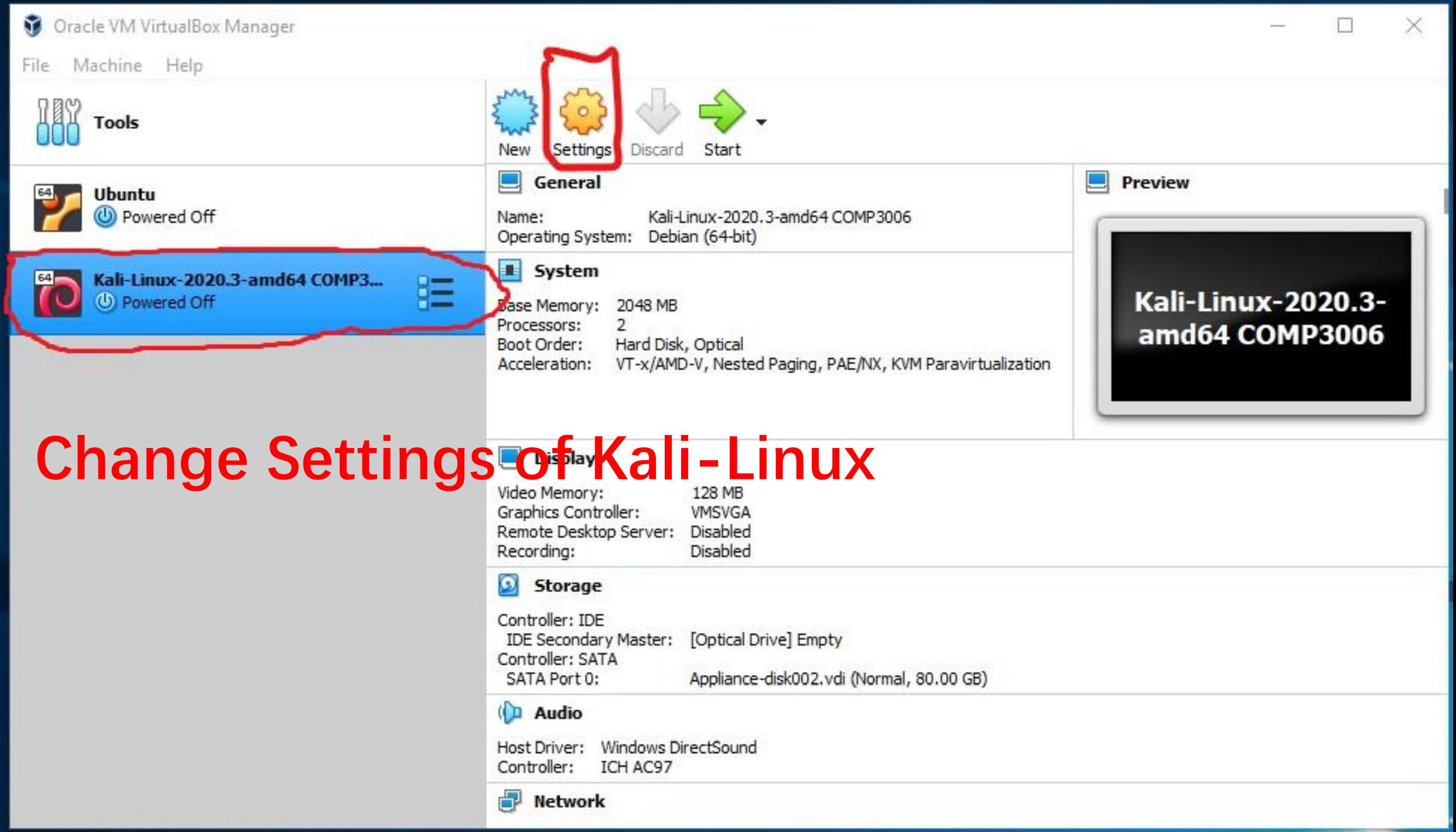

Import Virtual Appliance
Untick USB Controller
& Click Import
Appliance settings
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.
Virtual System 1
Name
Ubuntu
Description
Ubuntu 12 Server
Guest OS Type
Ubuntu (64-bit)
CPU
1
RAM
2048 MB
DVD
USB Controller
Sound Card
ICH AC97
Network Adapter
Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (IDE)
PIIX4
Storage Controller (IDE)
PIIX4
Storage Controller (SATA)
AHCI
Virtual Disk Image
Appliance-disk001.vmdk
Base Folder
C:\Users\z2020051\VirtualBox VMs
Primary Group
/
Virtual System 2
Name
Kali-Linux-2020.3-amd64 COMP3006
Untick Checkbox
Machine Base Folder:
C:\Users\z2020051\VirtualBox VMs
MAC Address Policy:
Include only NAT network adapter MAC addresses
Additional Options:
Import hard drives as VDI
Appliance is not signed
Restore Defaults
Import
Cancel


Importing –
May Take A Few Minutes
Import Virtual Appliance
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.
Name Ubuntu
Description Ubuntu 12 Server
Guest OS Type Ubuntu (64-bit)
CPU 1
RAM 2048 MB
DVD
USB Controller
Sound Card
Network Adapter
Storage Controller (IDE)
Storage Controller (IDE)
Storage Controller (SATA) AHCI
Virtual Disk Image Appliance-disk001.vmdk
Base Folder C:\Users\z2020051\VirtualBox VMs
Primary Group /
Virtual System 2
Name Kali-Linux-2020.3-amd64 COMP3006
Importing Appliance ...: Importing appliance 'C:\Security Lab\SEC...
Importing virtual disk image 'Appliance-disk001.vmdk' ... (2/5)
9%
1 minute, 18 seconds remaining
Machine Base Folder: C:\Users\z2020051\VirtualBox VMs
MAC Address Policy: Include only NAT network adapter MAC addresses
Additional Options: Import hard drives as VDI
Appliance is not signed
Restore Defaults
Import
Cancel

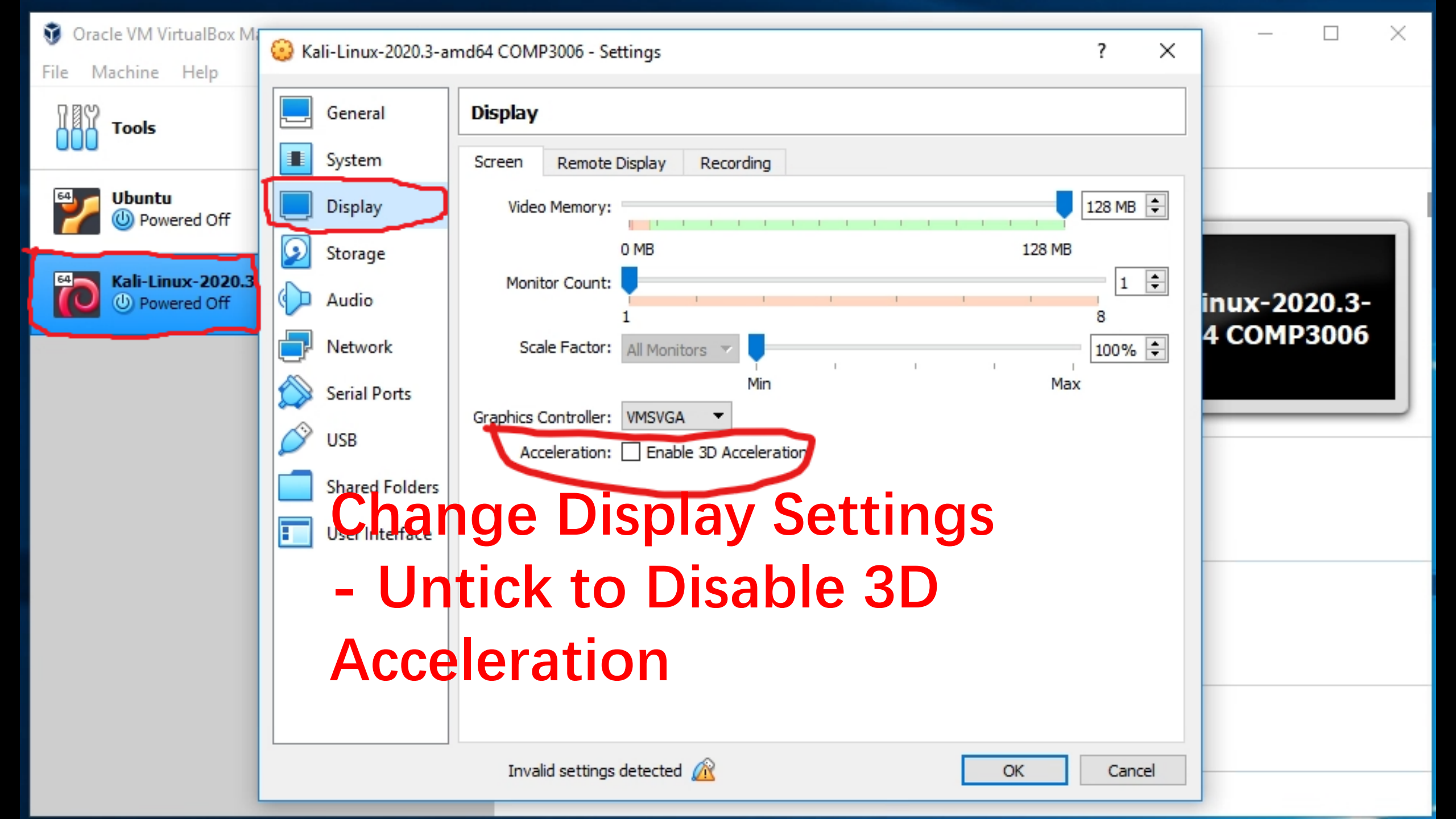

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Ubuntu
Powered Off
Kali-Linux-2020.3-amd64 COMP3...
Powered Off
New
Settings
Discard
Start
General
Name: Kali-Linux-2020.3-amd64 COMP3006
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Preview
Kali-Linux-2020.3-amd64 COMP3006
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Appliance-disk002.vdi (Normal, 80.00 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
Two Virtual Systems Imported - Ubuntu and Kali-Linux

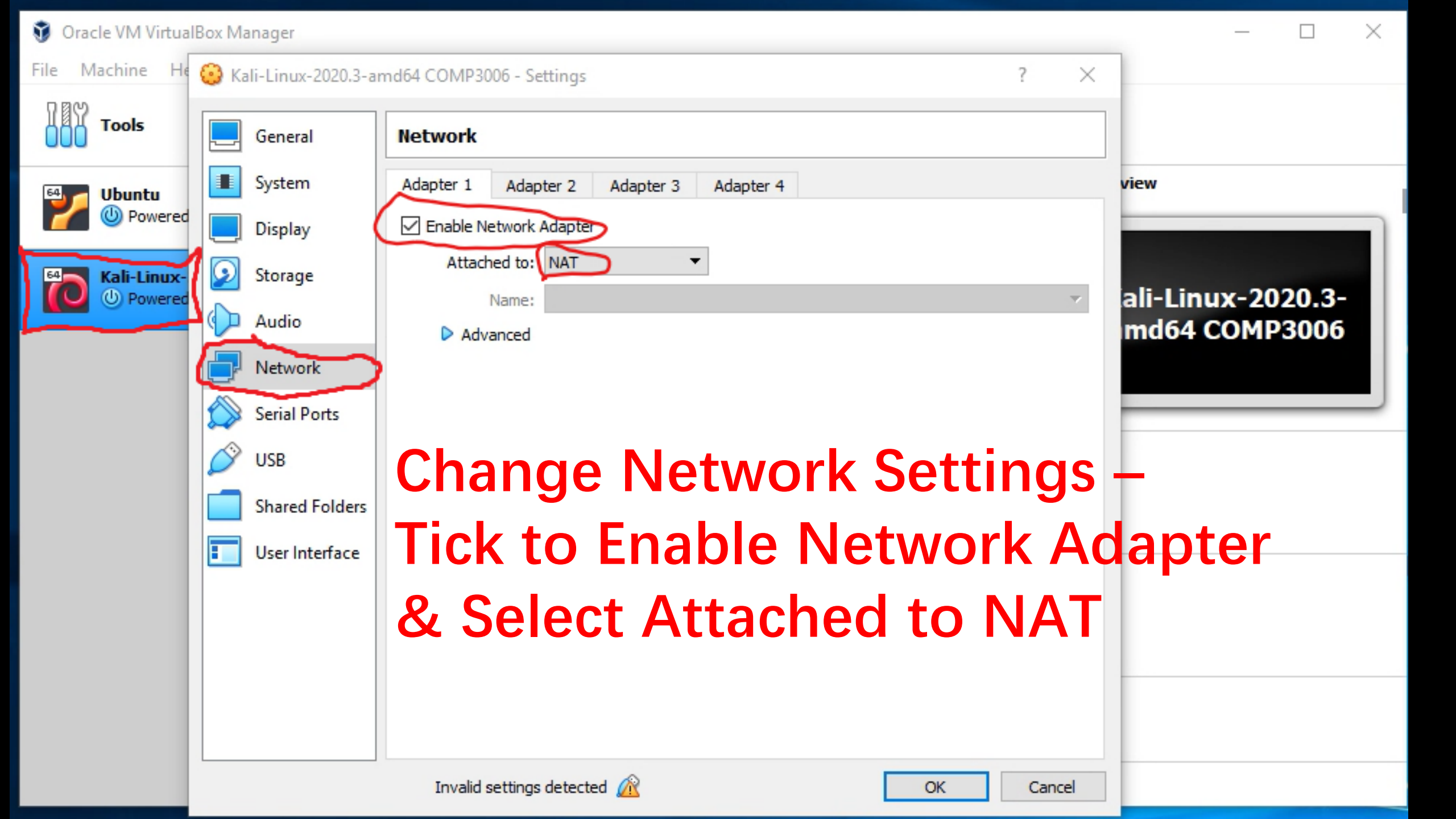
Configuring Kali-Linux Virtual Machine's Environment (1)

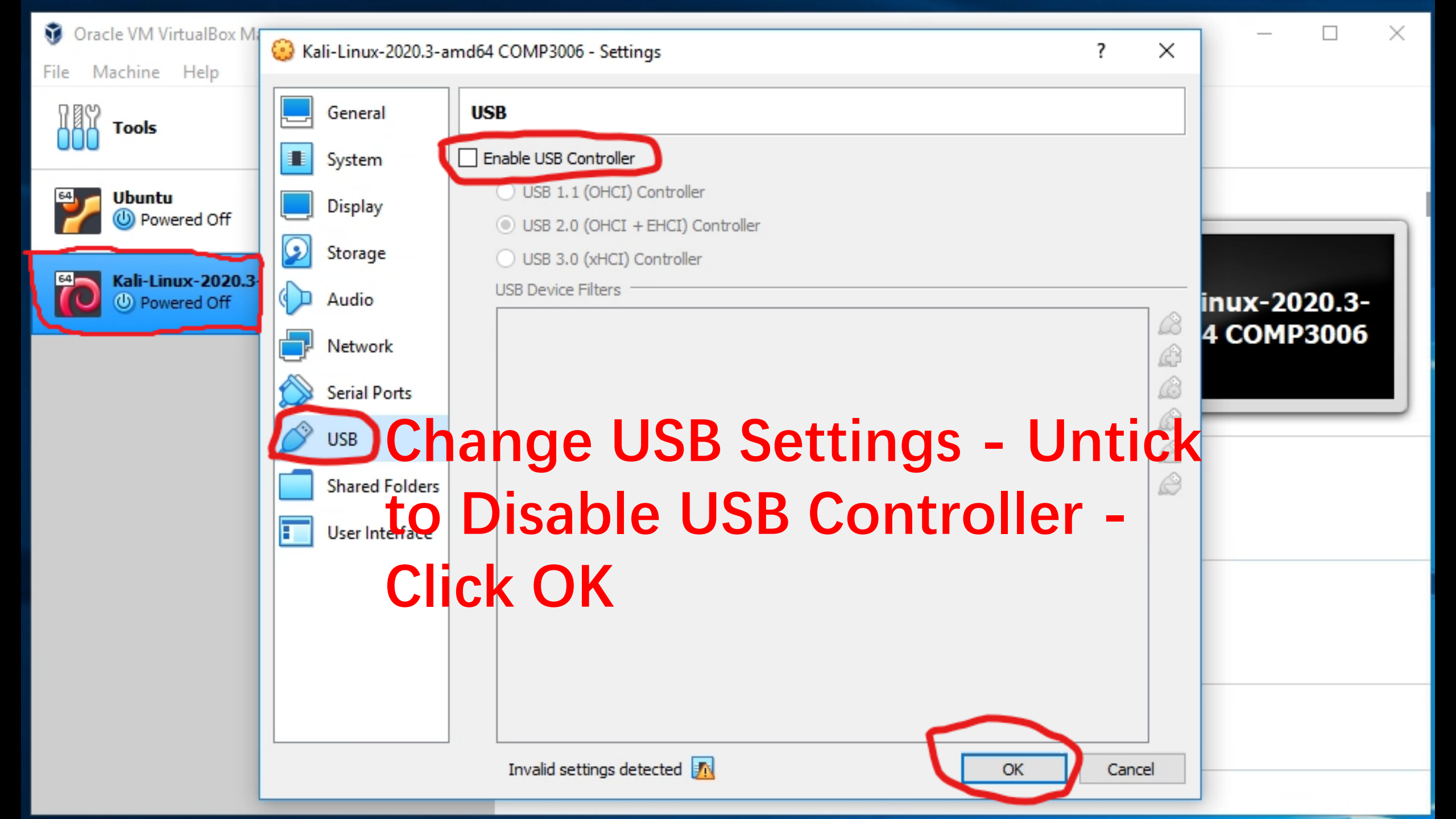
- You have successfully installed two virtual machines: Ubuntu and Kali-Linux.
- You will only use Kali-Linux in this and the next two lab sessions.
- You need to change some basic settings for the Kali-Linux virtual machine's environment (display, network, storage, etc..), as shown in the next few slides.



Change Settings of Kali-Linux

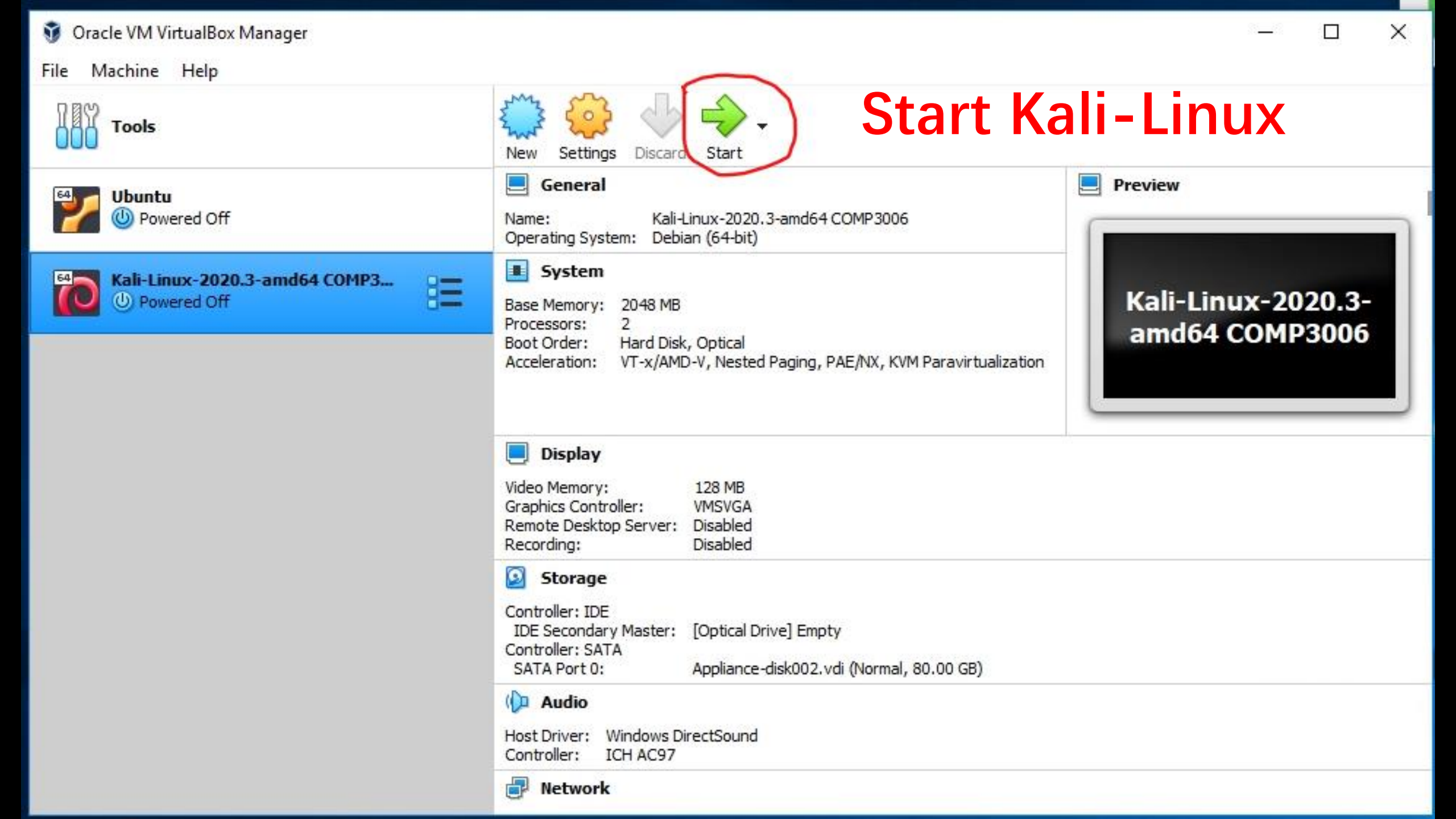

Oracle VM VirtualBox M
File Machine Help
Tools
Ubuntu
Powered Off
Kali-Linux-2020.3
Powered Off
Kali-Linux-2020.3-amd64 COMP3006 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Display
Screen
Remote Display
Recording
Video Memory:
128 MB
0 MB
128 MB
Monitor Count:
1
1
8
Scale Factor:
All Monitors
100%
Min
Max
Graphics Controller:
VMSVGA
Acceleration:
Enable 3D Acceleration
Invalid settings detected
OK
Cancel
inux-2020.3-
4 COMP3006
Change Display Settings
- Untick to Disable 3D
Acceleration

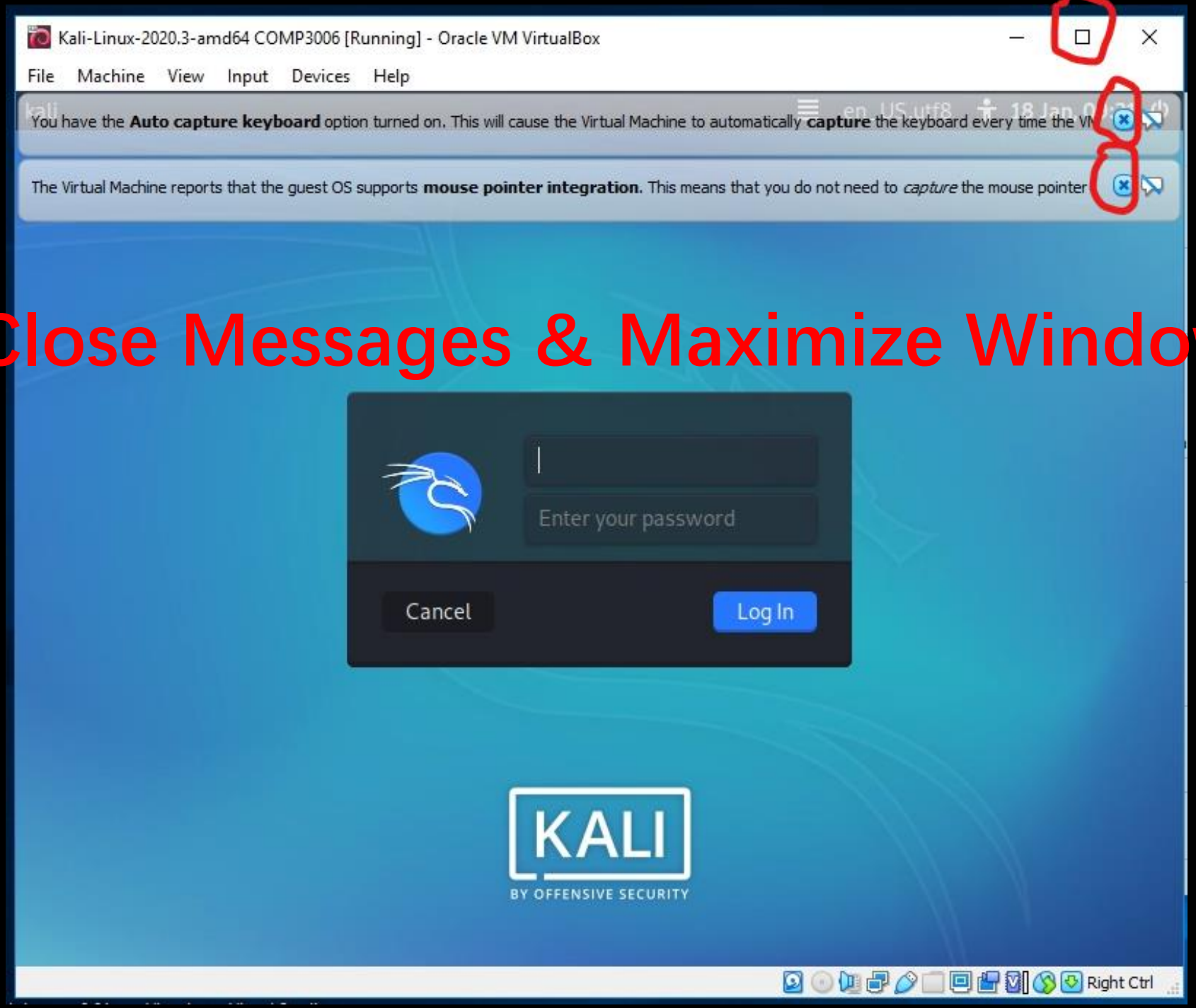

Oracle VM VirtualBox Manager
File
Machine
Tools
Ubuntu
Powered
Kali-Linux-
Powered
Kali-Linux-2020.3-amd64 COMP3006 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
NAT
Name:
Advanced
Invalid settings detected
OK
Cancel
Change Network Settings –
Tick to Enable Network Adapter
& Select Attached to NAT

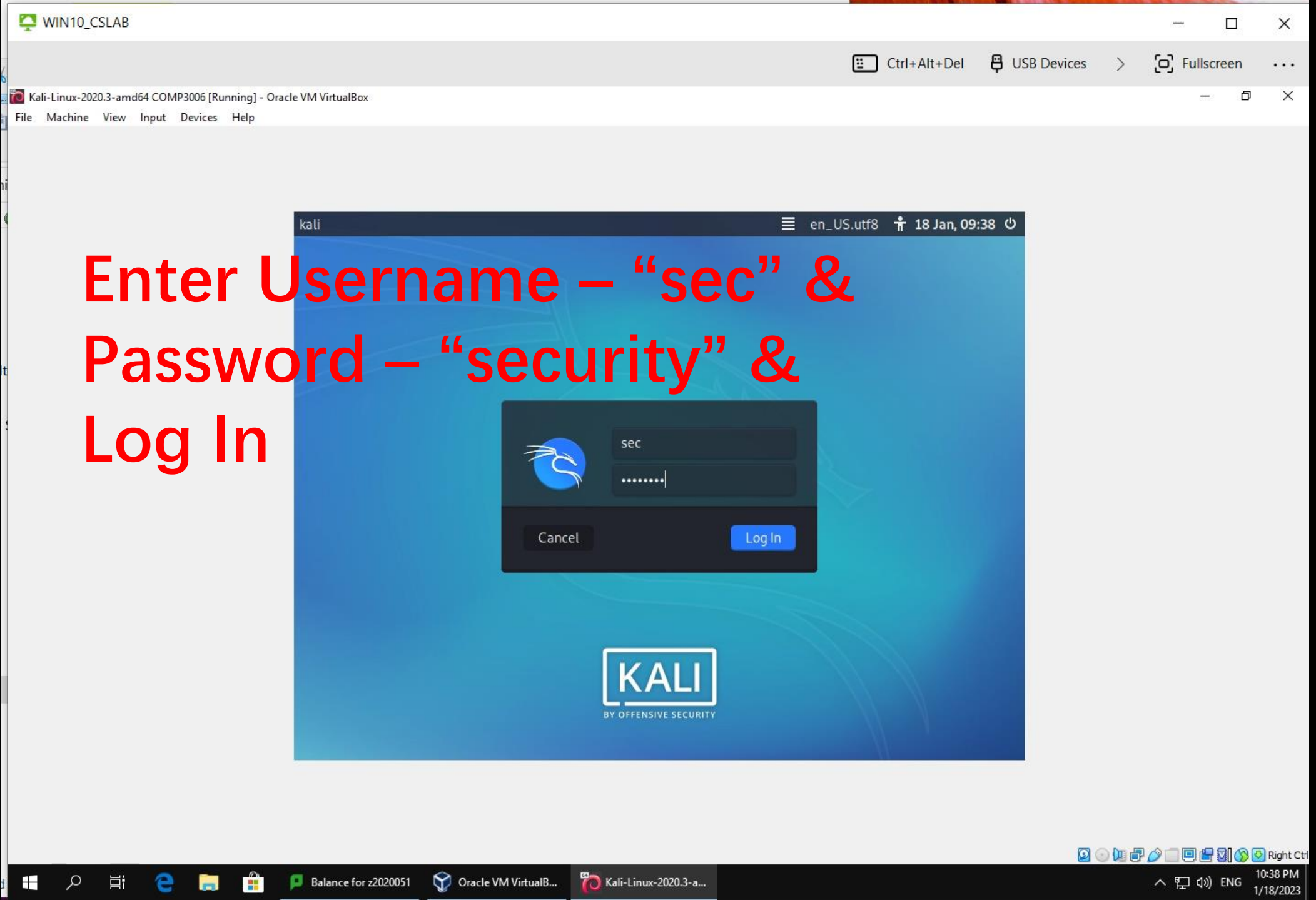

Oracle VM VirtualBox Ma
File Machine Help
Tools
Ubuntu
Powered Off
Kali-Linux-2020.3-
Powered Off
Kali-Linux-2020.3-amd64 COMP3006 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
USB
Enable USB Controller
USB 1.1 (OHCI) Controller
USB 2.0 (OHCI + EHCI) Controller
USB 3.0 (xHCI) Controller
USB Device Filters
Invalid settings detected
OK
Cancel
inux-2020.3-
4 COMP3006
Change USB Settings - Untick
to Disable USB Controller -
Click OK

Configuring Kali-Linux Virtual Machine's Environment (2)

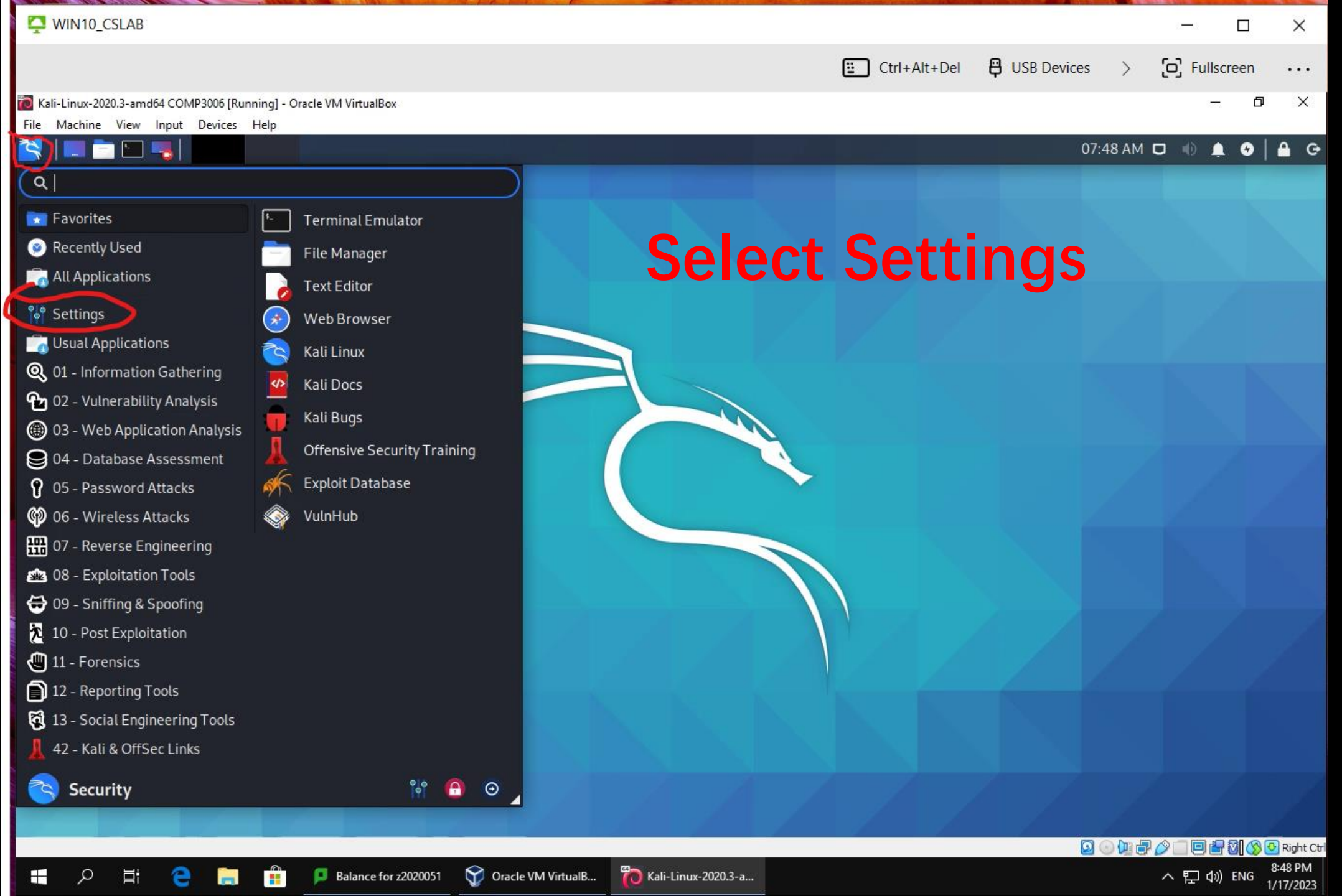
- Your next task is to log in to the Kali-Linux virtual machine account, which has been created for you when you did the installation and configuration using the OVA file called SEC2021VMs.
- Your username is "sec" and your sign-in password is "security".
- You will be brought into the GUI environment of the Kali-Linux virtual operating system.
- You need to do an additional setting about the Kali-Linux's environment (i.e., keyboard layout).
- You will then switch to the command-line mode, in which you will do most of your lab exercises.

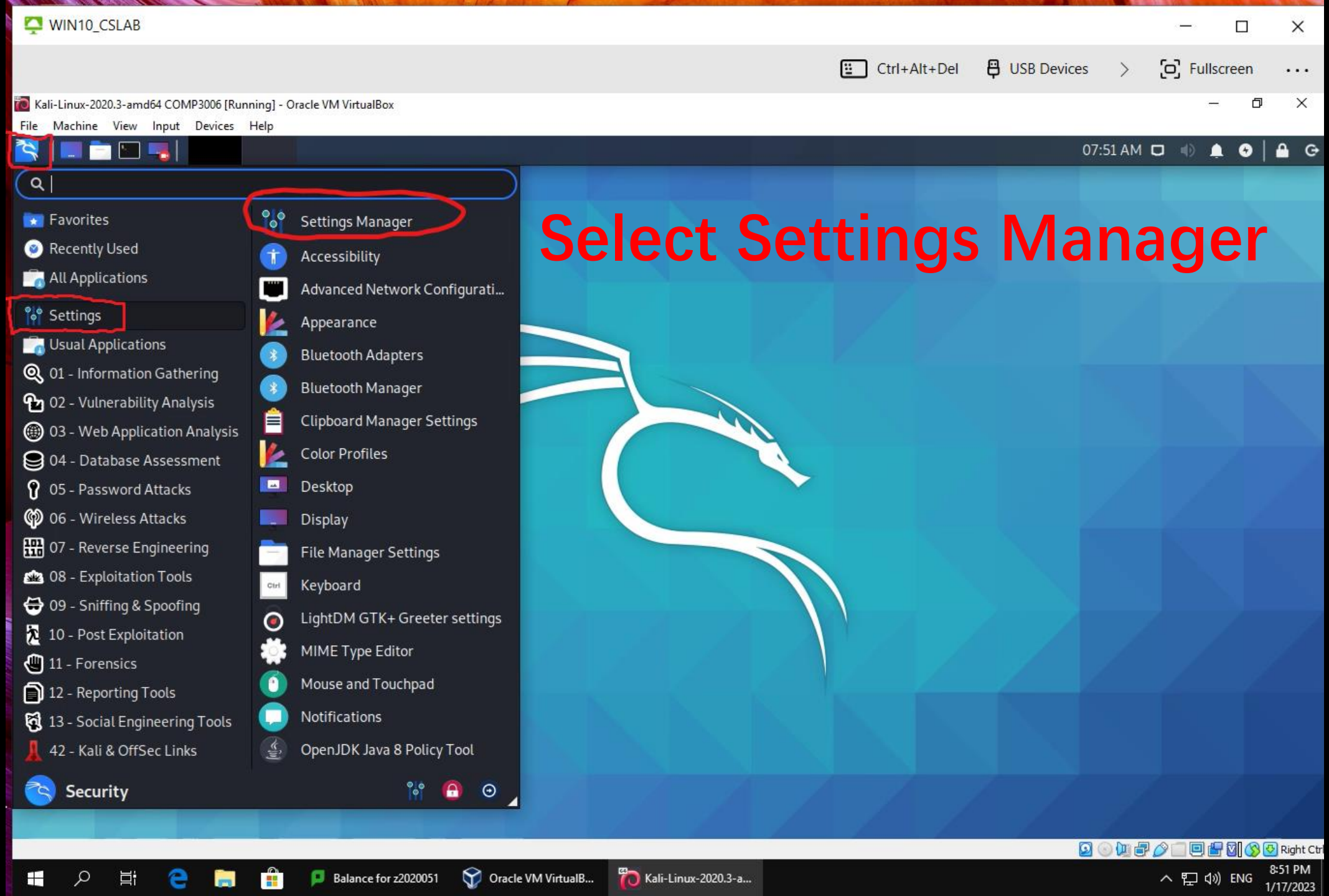

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Settings
Discard
Start
Start Kali-Linux
Ubuntu
Powered Off
Kali-Linux-2020.3-amd64 COMP3...
Powered Off
General
Name: Kali-Linux-2020.3-amd64 COMP3006
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Preview
Kali-Linux-2020.3-amd64 COMP3006
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Appliance-disk002.vdi (Normal, 80.00 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network

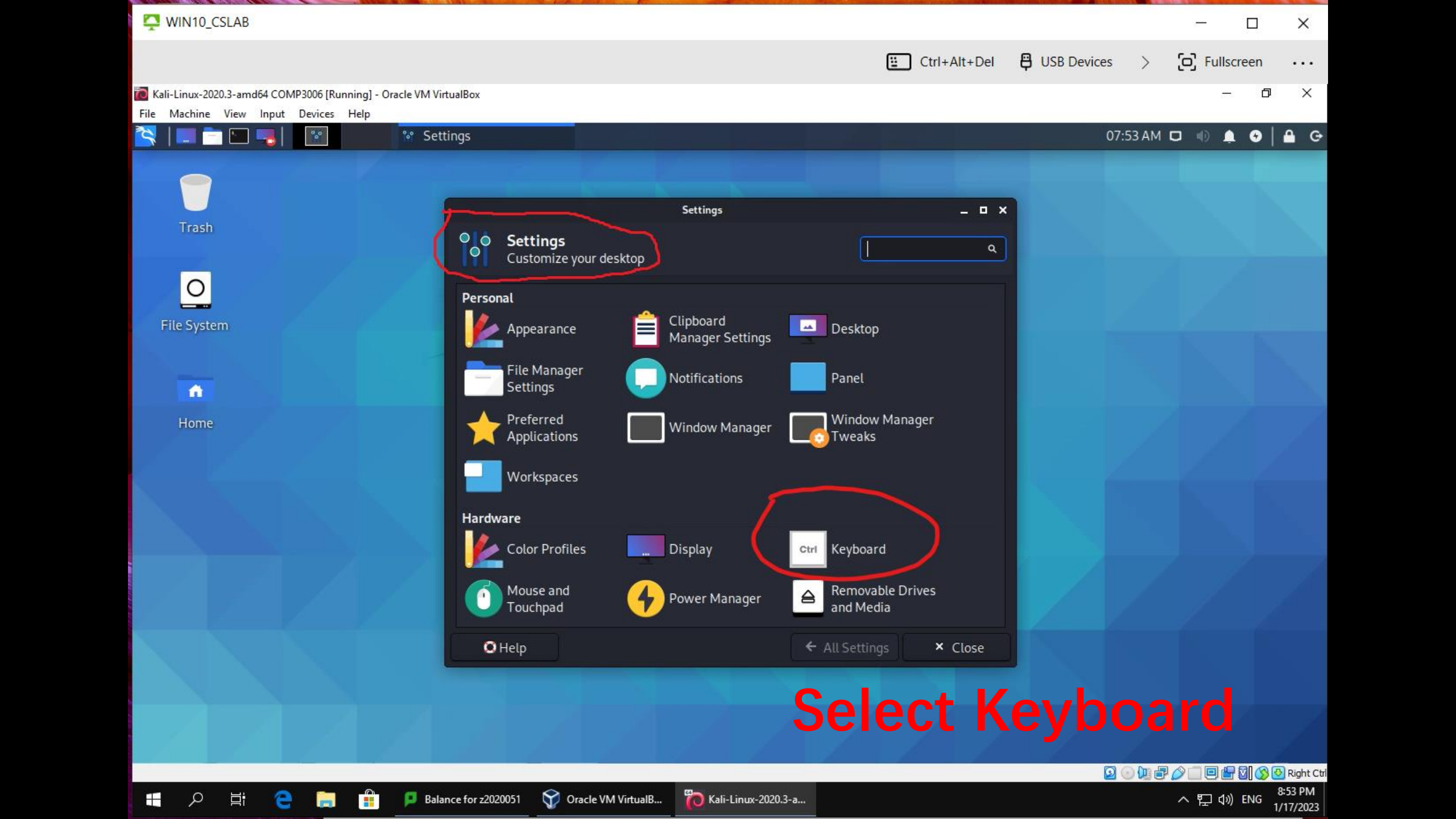

Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer
Close Messages & Maximize Window
Enter your password
Cancel
Log In
KALI
BY OFFENSIVE SECURITY
Right Ctrl

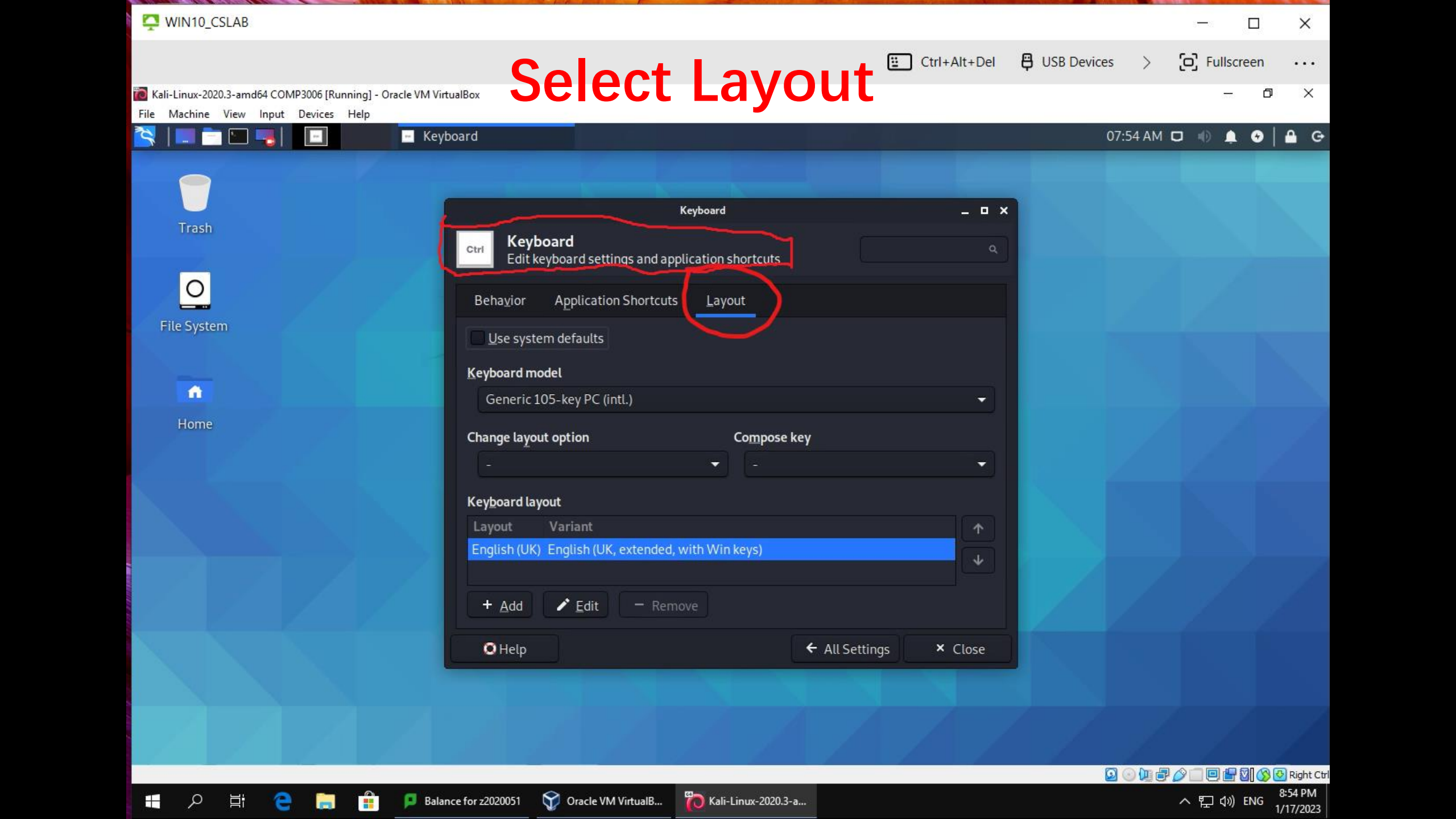

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali
en_US.utf8
18 Jan, 09:38
Enter Username – “sec” &
Password – “security” &
Log In
sec
Cancel
Log In
KALI
BY OFFENSIVE SECURITY
Right Ctrl
Balance for z2020051
Oracle VM VirtualB...
Kali-Linux-2020.3-a...
ENG
10:38 PM
1/18/2023

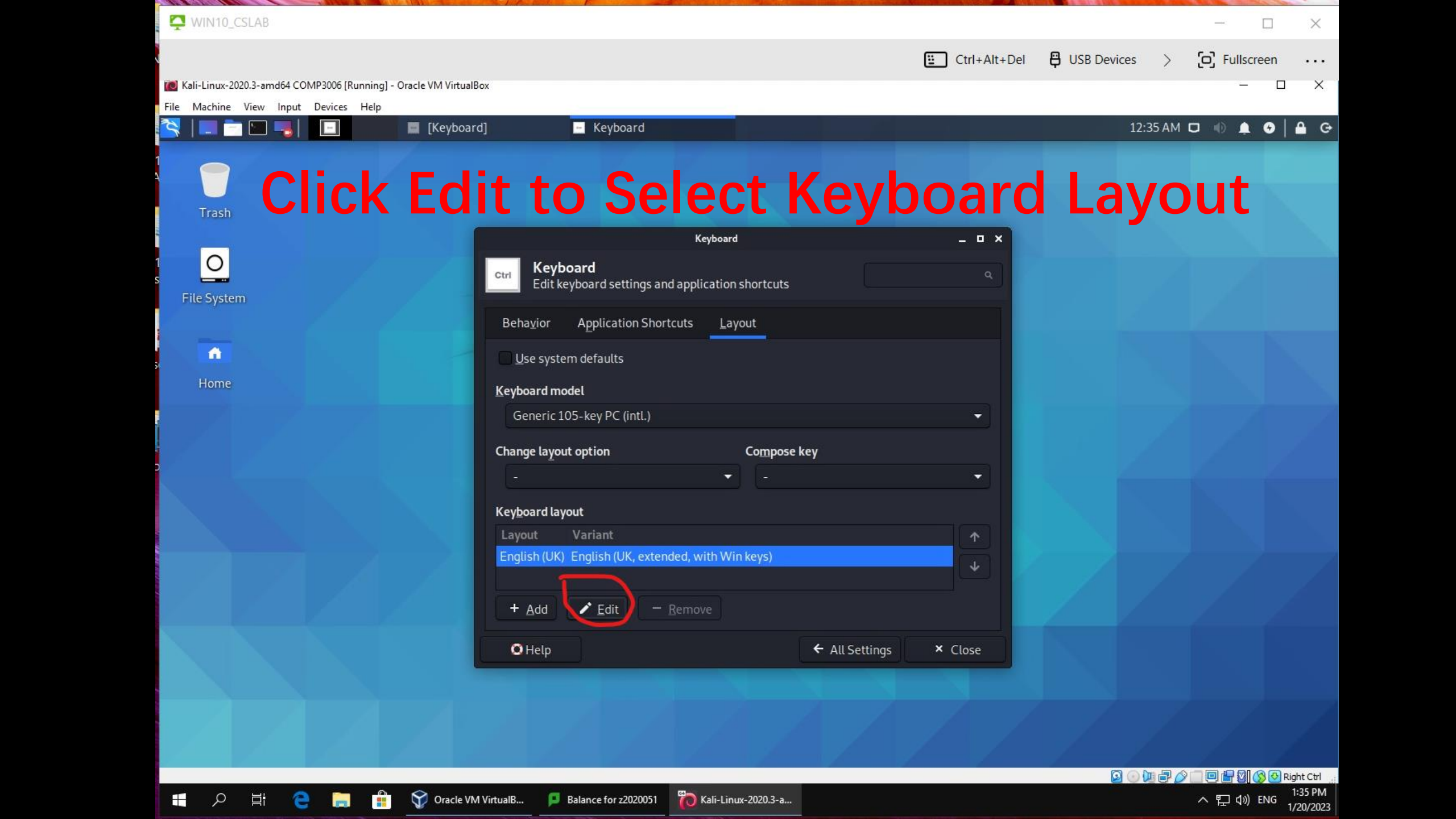

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
07:46 AM
Trash
File System
Home
To Change Keyboard Layout
- Click Kali Menu Button
Right Ctrl
Balance for z2020051
Oracle VM VirtualB...
Kali-Linux-2020.3-a...
ENG
8:46 PM
1/17/2023

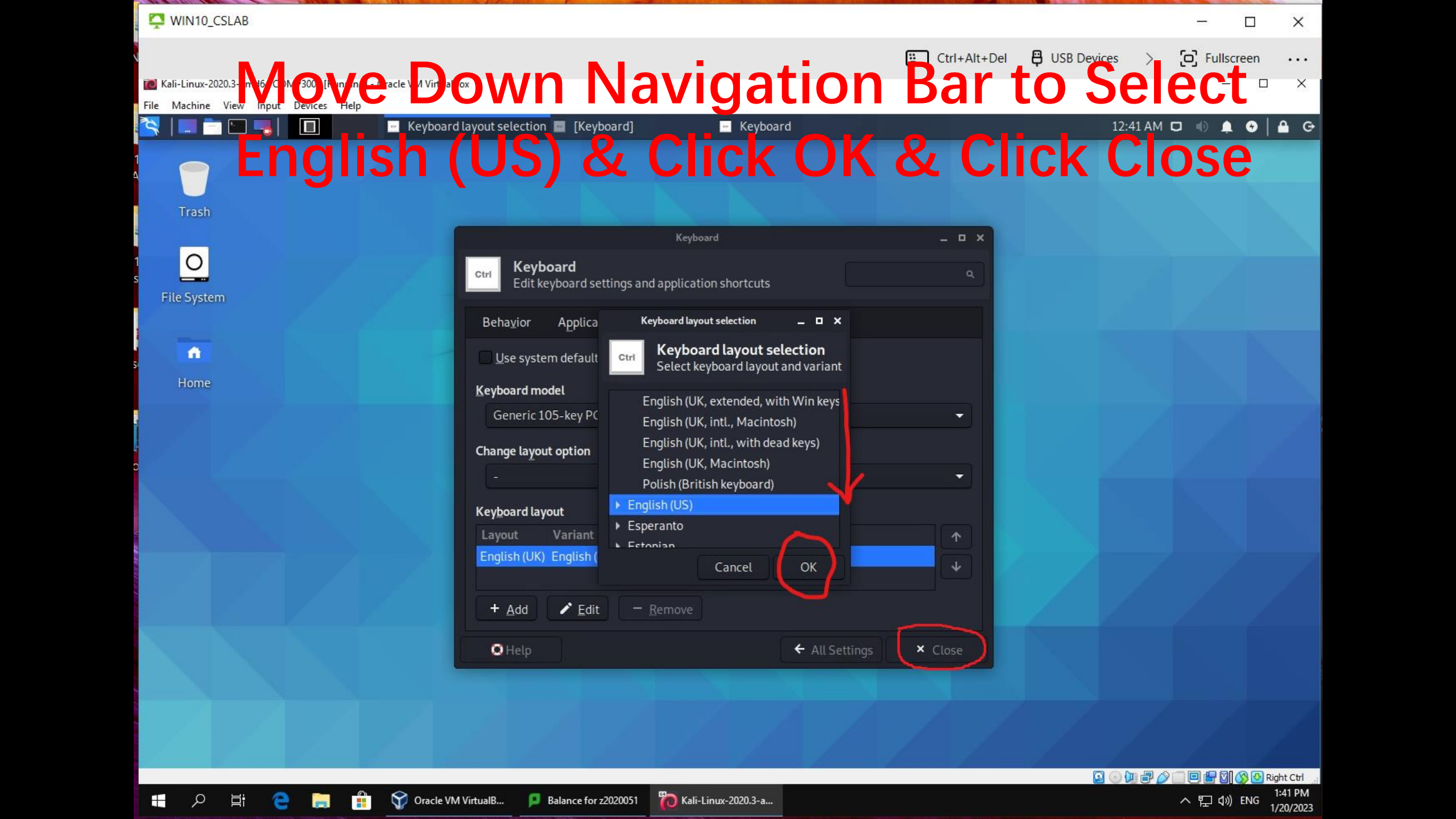

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
07:48 AM
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
Terminal Emulator
File Manager
Text Editor
Web Browser
Kali Linux
Kali Docs
Kali Bugs
Offensive Security Training
Exploit Database
VulnHub
Security
Select Settings
Right Ctrl
Balance for z2020051
Oracle VM VirtualB...
Kali-Linux-2020.3-a...
ENG
8:48 PM
1/17/2023

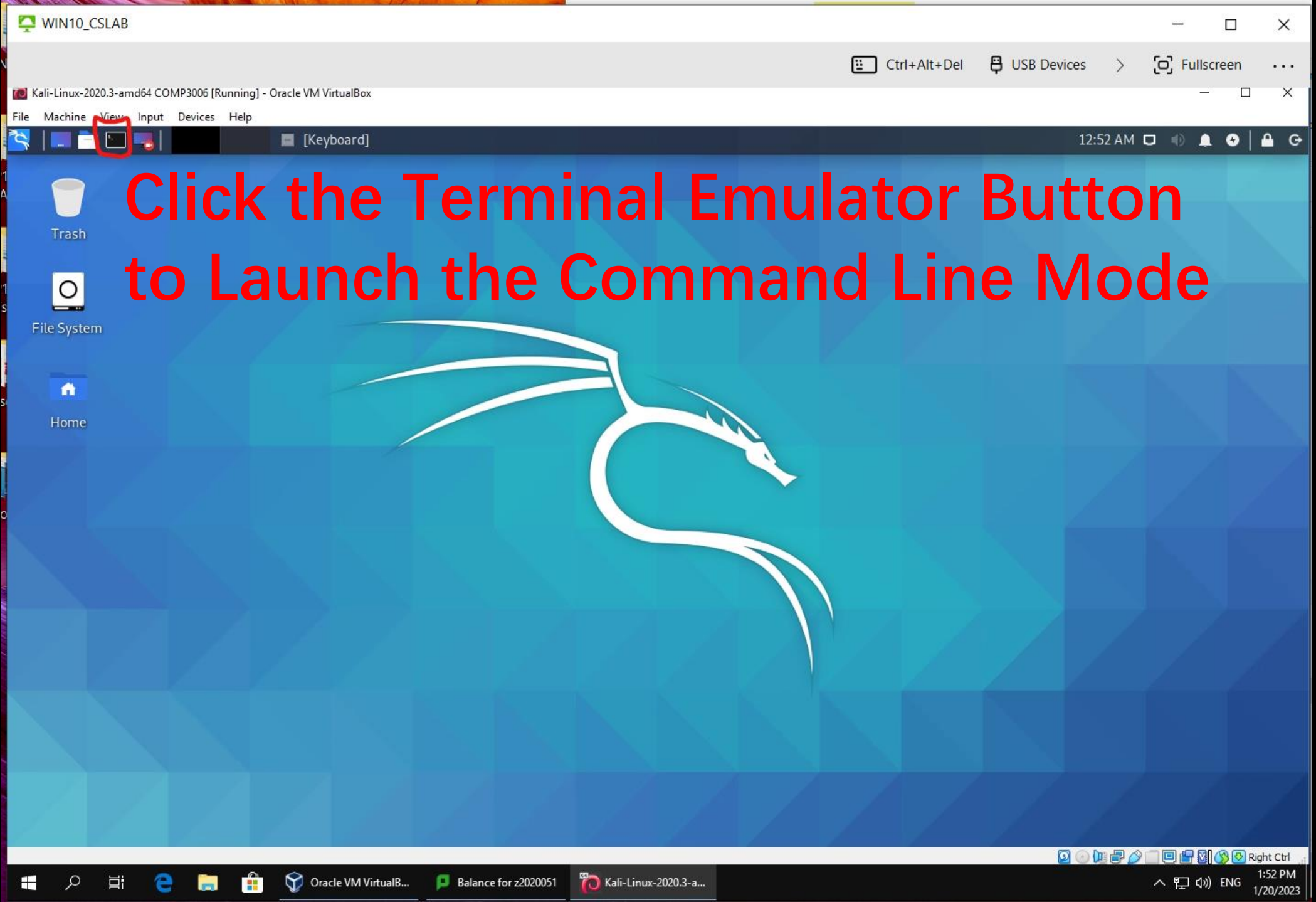

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
07:51 AM
Select Settings Manager
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
Security
Settings Manager
Accessibility
Advanced Network Configurati...
Appearance
Bluetooth Adapters
Bluetooth Manager
Clipboard Manager Settings
Color Profiles
Desktop
Display
File Manager Settings
Keyboard
LightDM GTK+ Greeter settings
MIME Type Editor
Mouse and Touchpad
Notifications
OpenJDK Java 8 Policy Tool
Right Ctrl
Balance for z2020051
Oracle VM VirtualB...
Kali-Linux-2020.3-a...
ENG
8:51 PM
1/17/2023

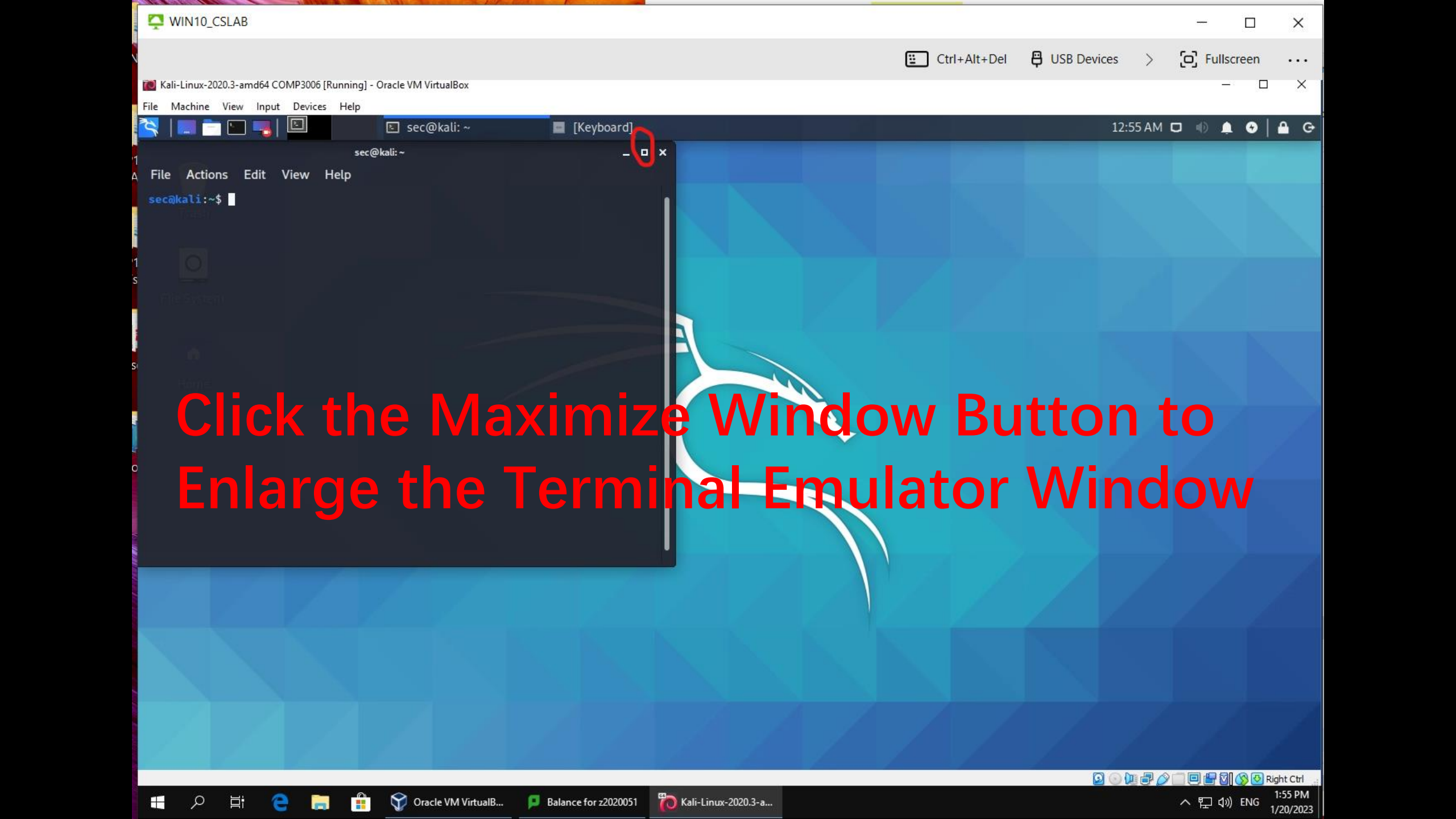

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Settings
07:53 AM
Trash
File System
Home
Settings
Settings
Customize your desktop
Personal
Appearance
Clipboard Manager Settings
Desktop
File Manager Settings
Notifications
Panel
Preferred Applications
Window Manager
Window Manager Tweaks
Workspaces
Hardware
Color Profiles
Display
Keyboard
Mouse and Touchpad
Power Manager
Removable Drives and Media
Help
All Settings
Close
Select Keyboard
Right Ctrl
Balance for z2020051
Oracle VM VirtualB...
Kali-Linux-2020.3-a...
ENG
8:53 PM
1/17/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Select Layout
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Keyboard
07:54 AM
Trash
File System
Home
Keyboard
Ctrl
Keyboard
Edit keyboard settings and application shortcuts
Behavior
Application Shortcuts
Layout
Use system defaults
Keyboard model
Generic 105-key PC (intl.)
Change layout option
Compose key
Keyboard layout
Layout
Variant
English (UK)
English (UK, extended, with Win keys)
Add
Edit
Remove
Help
All Settings
Close
Right Ctrl
Balance for z2020051
Oracle VM VirtualB...
Kali-Linux-2020.3-a...
ENG
8:54 PM
1/17/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[Keyboard]
Keyboard
12:35 AM
Click Edit to Select Keyboard Layout
Trash
File System
Home
Keyboard
Keyboard
Edit keyboard settings and application shortcuts
Behavior
Application Shortcuts
Layout
Use system defaults
Keyboard model
Generic 105-key PC (intl.)
Change layout option
Compose key
Keyboard layout
Layout
Variant
English (UK)
English (UK, extended, with Win keys)
Add
Edit
Remove
Help
All Settings
Close
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
1:35 PM
1/20/2023

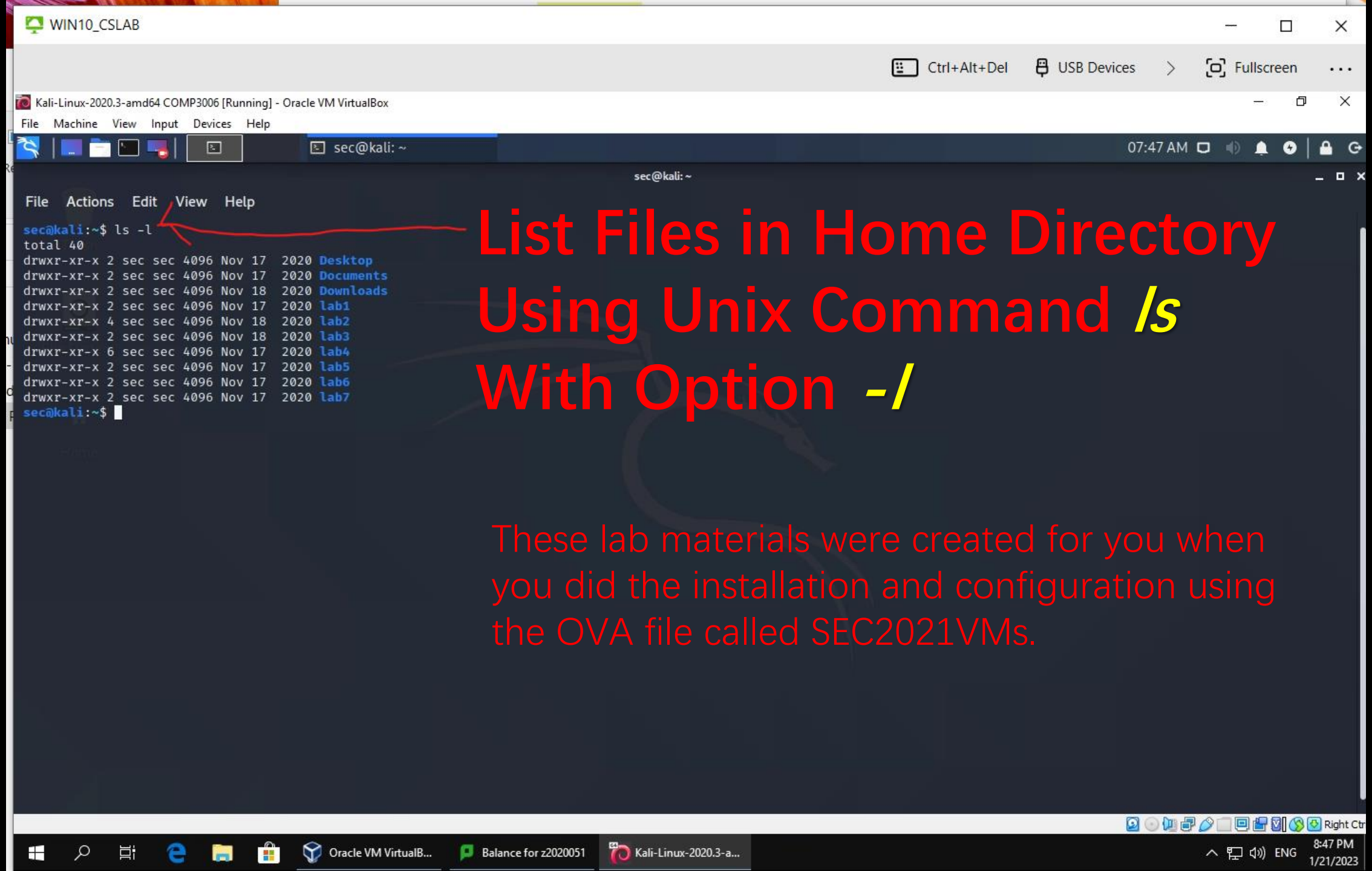

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Move Down Navigation Bar to Select
English (US) & Click OK & Click Close
File Machine View Input Devices Help
Keyboard layout selection
[Keyboard]
Keyboard
12:41 AM
Trash
File System
Home
Keyboard
Keyboard
Edit keyboard settings and application shortcuts
Behavior
Applica
Use system default
Keyboard model
Generic 105-key PC
Change layout option
Keyboard layout
Layout
Variant
English (UK)
English (
Add
Edit
Remove
Help
All Settings
Close
Keyboard layout selection
Keyboard layout selection
Select keyboard layout and variant
English (UK, extended, with Win keys
English (UK, intl., Macintosh)
English (UK, intl., with dead keys)
English (UK, Macintosh)
Polish (British keyboard)
English (US)
Esperanto
Cancel
OK
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
1:41 PM
1/20/2023

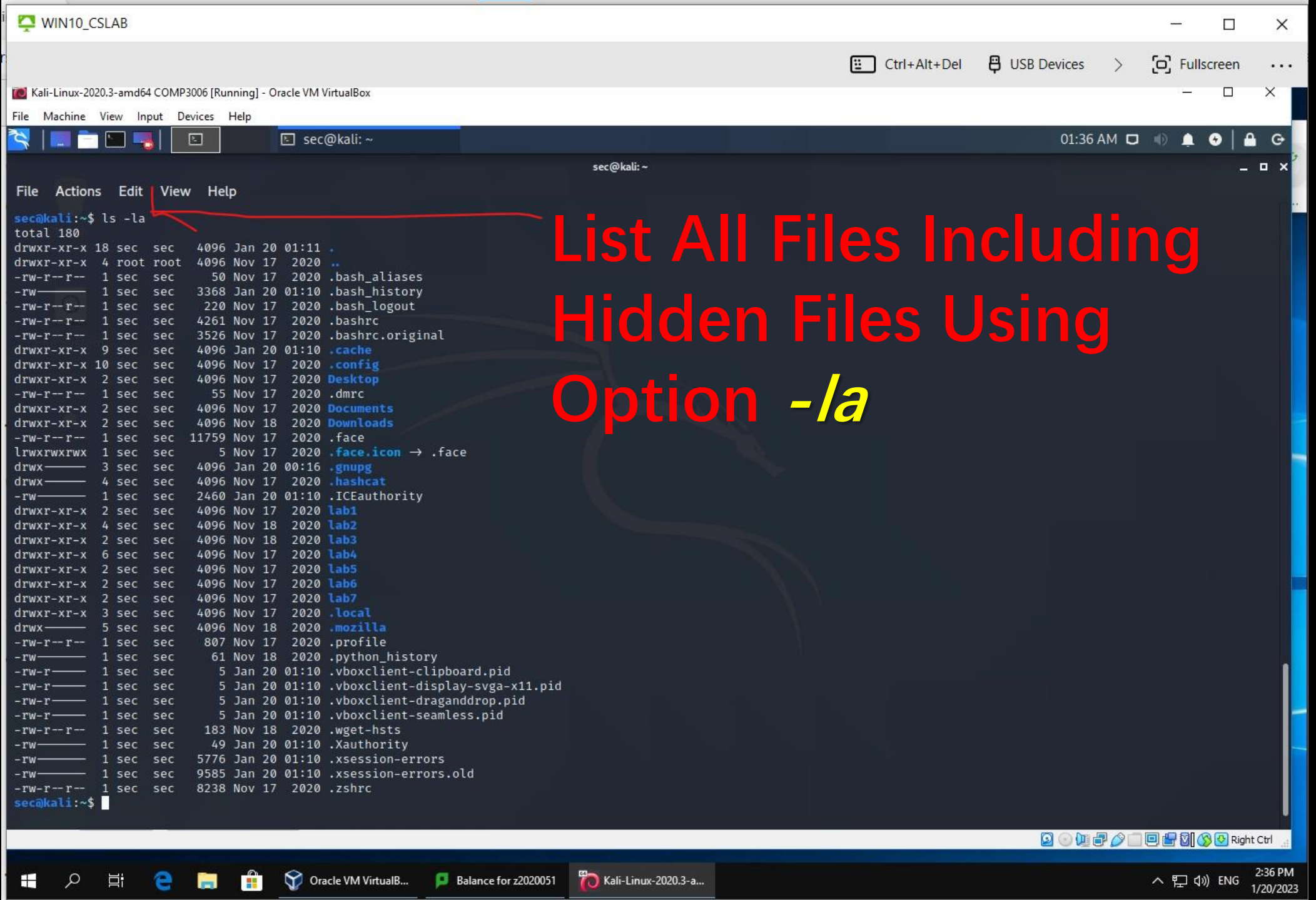

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[Keyboard]
12:52 AM
Trash
File System
Home
Click the Terminal Emulator Button
to Launch the Command Line Mode
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
1:52 PM
1/20/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~
[Keyboard]
12:55 AM
sec@kali: ~
File Actions Edit View Help
sec@kali:~$
Click the Maximize Window Button to Enlarge the Terminal Emulator Window
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
1:55 PM
1/20/2023

Learning Computer Security Based on Kali-Linux

- Let's begin our journey of Computer Security based on Kali-Linux.
- Kali-Linux is one of the most popular platforms for learning Cybersecurity and Ethical Hacking.
- We assume that you have some background knowledge on Unix, or more specifically, Linux, before starting this module.
- You may refer to the following website for some basic commands:
  50 Basic Linux Commands you Need to Know on Kali Linux
  https://infosecscout.com/basic-kali-linux-commands/


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~
07:47 AM
sec@kali: ~
File Actions Edit View Help
sec@kali:~$ ls -l
total 40
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
sec@kali:~$
List Files in Home Directory
Using Unix Command ls
With Option -l
These lab materials were created for you when you did the installation and configuration using the OVA file called SEC2021VMs.
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
8:47 PM
1/21/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~
01:36 AM
sec@kali: ~
File Actions Edit View Help
sec@kali:~$ ls -la
total 180
drwxr-xr-x 18 sec sec 4096 Jan 20 01:11 .
drwxr-xr-x 4 root root 4096 Nov 17 2020 ..
-rw-r--r-- 1 sec sec 50 Nov 17 2020 .bash_aliases
-rw------- 1 sec sec 3368 Jan 20 01:10 .bash_history
-rw-r--r-- 1 sec sec 220 Nov 17 2020 .bash_logout
-rw-r--r-- 1 sec sec 4261 Nov 17 2020 .bashrc
-rw-r--r-- 1 sec sec 3526 Nov 17 2020 .bashrc.original
drwxr-xr-x 9 sec sec 4096 Jan 20 01:10 .cache
drwxr-xr-x 10 sec sec 4096 Nov 17 2020 .config
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
-rw-r--r-- 1 sec sec 55 Nov 17 2020 .dmrc
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rw-r--r-- 1 sec sec 11759 Nov 17 2020 .face
lrwxrwxrwx 1 sec sec 5 Nov 17 2020 .face.icon → .face
drwx------ 3 sec sec 4096 Jan 20 00:16 .gnupg
drwx------ 4 sec sec 4096 Nov 17 2020 .hashcat
-rw------- 1 sec sec 2460 Jan 20 01:10 .ICEauthority
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
drwxr-xr-x 3 sec sec 4096 Nov 17 2020 .local
drwx------ 5 sec sec 4096 Nov 18 2020 .mozilla
-rw-r--r-- 1 sec sec 807 Nov 17 2020 .profile
-rw------- 1 sec sec 61 Nov 18 2020 .python_history
-rw-r----- 1 sec sec 5 Jan 20 01:10 .vboxclient-clipboard.pid
-rw-r----- 1 sec sec 5 Jan 20 01:10 .vboxclient-display-svga-x11.pid
-rw-r----- 1 sec sec 5 Jan 20 01:10 .vboxclient-draganddrop.pid
-rw-r----- 1 sec sec 5 Jan 20 01:10 .vboxclient-seamless.pid
-rw-r--r-- 1 sec sec 183 Nov 18 2020 .wget-hsts
-rw------- 1 sec sec 49 Jan 20 01:10 .Xauthority
-rw------- 1 sec sec 5776 Jan 20 01:10 .xsession-errors
-rw------- 1 sec sec 9585 Jan 20 01:10 .xsession-errors.old
-rw-r--r-- 1 sec sec 8238 Nov 17 2020 .zshrc
sec@kali:~$
List All Files Including Hidden Files Using Option -la
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
2:36 PM
1/20/2023

Access Control and Super User Privilege

- Access control is an important measure in computer security. It controls who has the right to do what within a system.
- An operating system, such as Kali-Linux, records the activities/transactions of the users in a system log file called “syslog”. We can then perform some analysis related to computer security based on the transactions recorded in the log file.
- An ordinary user is not allowed to access “syslog”, unless he/she is elevated to the level of a super user using “sudo” command.
- An additional “elevation” step is to ensure accountability and non-repudiation by explicitly recording the request for a super user privilege.

Access Control and Super User Privilege

- You will use the “cat” command to display the content (i.e., transactions/lines) of the log file.
- You will use the “grep” command to search for a keyword, and to display the transactions/lines in the log file containing the keyword.
- You will use the “|” (i.e., pipe) command to feed the output from a “cat” command as the input to a “grep” command. This process is called piping.
- You will use the “wc” command to count and display the total number of transactions/lines in a file.
- You will use the “>” command to redirect an output to a file.

Display System Logs with sudo Privilege & Enter Password *security*

WIN10_CSLAB

Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

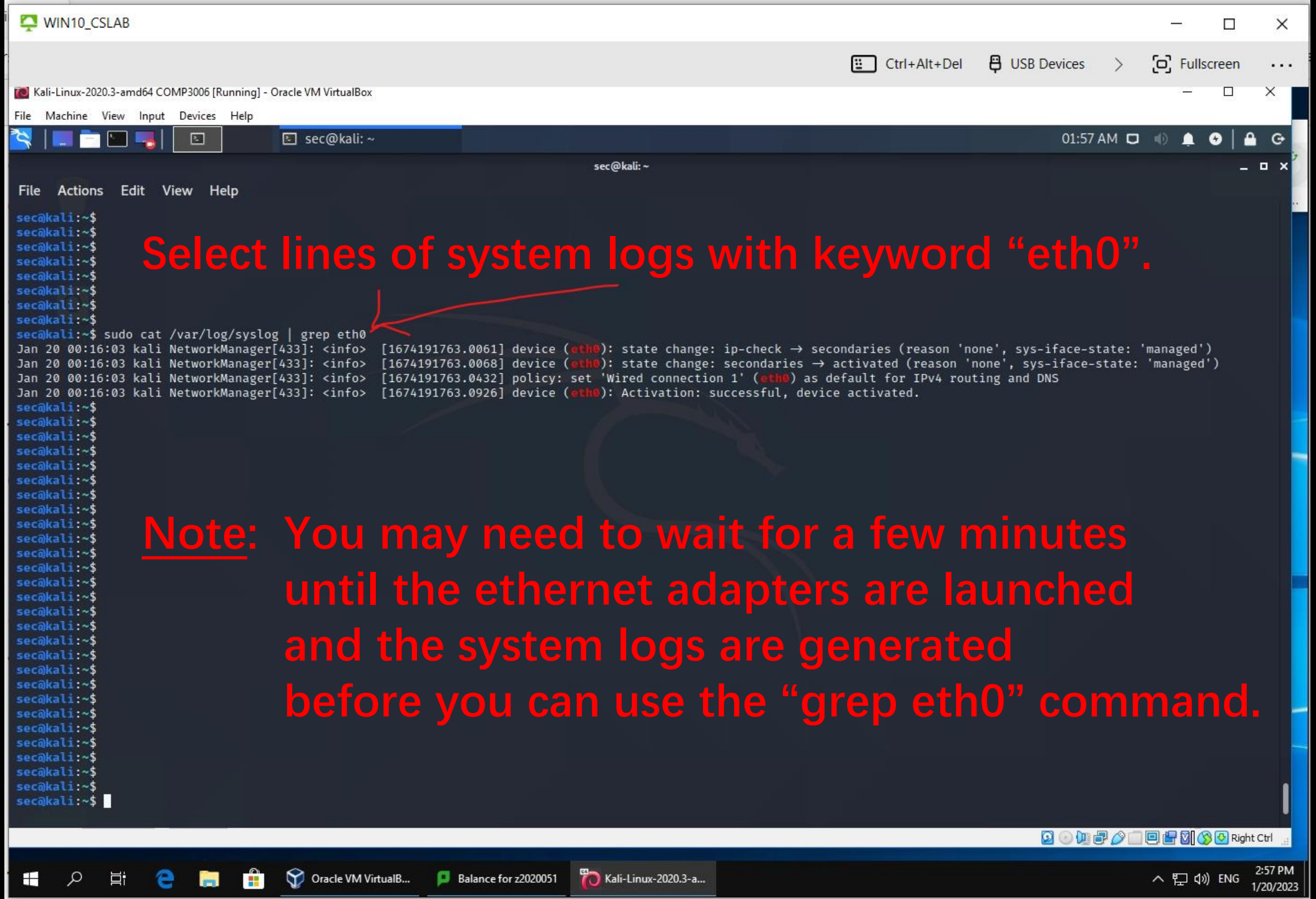
File Actions Edit View Help

```
sec@kali:~$
sec@kali:~$
sec@kali:~$
sec@kali:~$ sudo cat /var/log/syslog
[sudo] password for sec:
Jan 20 00:16:03 kali NetworkManager[433]: <info>  [1674191763.0061] device (eth0): state change: ip-check → secondaries (reason 'none', sys-iface-state: 'managed')
Jan 20 00:16:03 kali NetworkManager[433]: <info>  [1674191763.0068] device (eth0): state change: secondaries → activated (reason 'none', sys-iface-state: 'managed')
Jan 20 00:16:03 kali rsyslogd: [origin software="rsyslogd" swVersion="8.2006.0" x-pid="438" x-info="https://www.rsyslog.com"] rsyslogd was HUPed
Jan 20 00:16:03 kali NetworkManager[433]: <info>  [1674191763.0336] manager: NetworkManager state is now CONNECTED_LOCAL
Jan 20 00:16:03 kali NetworkManager[433]: <info>  [1674191763.0422] manager: NetworkManager state is now CONNECTED_SITE
Jan 20 00:16:03 kali NetworkManager[433]: <info>  [1674191763.0432] policy: set 'Wired connection 1' (eth0) as default for IPv4 routing and DNS
Jan 20 00:16:03 kali dbus-daemon[432]: [system] Activating via systemd: service name='org.freedesktop.resolve1' unit='dbus-org.freedesktop.resolve1.service' requested by ':
1.2' (uid=0 pid=433 comm="/usr/sbin/NetworkManager --no-daemon ")
Jan 20 00:16:03 kali dbus-daemon[432]: [system] Activation via systemd failed for unit 'dbus-org.freedesktop.resolve1.service': Unit dbus-org.freedesktop.resolve1.service n
ot found.
Jan 20 00:16:03 kali systemd[1]: logrotate.service: Succeeded.
Jan 20 00:16:03 kali systemd[1]: Finished Rotate log files.
Jan 20 00:16:03 kali NetworkManager[433]: <info>  [1674191763.0926] device (eth0): Activation: successful, device activated.
Jan 20 00:16:03 kali NetworkManager[433]: <info>  [1674191763.0950] manager: NetworkManager state is now CONNECTED_GLOBAL
Jan 20 00:16:03 kali NetworkManager[433]: <info>  [1674191763.0962] manager: startup complete
Jan 20 00:16:06 kali systemd[1]: man-db.service: Succeeded.
Jan 20 00:16:06 kali systemd[1]: Finished Daily man-db regeneration.
Jan 20 00:16:06 kali systemd[1]: Startup finished in 8.971s (kernel) + 16.268s (userspace) = 25.239s.
Jan 20 00:16:06 kali lightdm[687]: Error getting user list from org.freedesktop.Accounts: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.freedesktop.Ac
counts was not provided by any .service files
Jan 20 00:16:06 kali systemd[1]: Created slice User Slice of UID 131.
Jan 20 00:16:06 kali systemd[1]: Starting User Runtime Directory /run/user/131...
Jan 20 00:16:06 kali systemd[1]: Finished User Runtime Directory /run/user/131.
Jan 20 00:16:06 kali systemd[1]: Starting User Manager for UID 131...
Jan 20 00:16:07 kali systemd[696]: gpgconf: error running '/usr/lib/gnupg/scdaemon': probably not installed
Jan 20 00:16:07 kali systemd[691]: Reached target Paths.
Jan 20 00:16:07 kali systemd[691]: Reached target Timers.
Jan 20 00:16:07 kali systemd[691]: Starting D-Bus User Message Bus Socket.
Jan 20 00:16:07 kali systemd[691]: Listening on GnuPG network certificate management daemon.
Jan 20 00:16:07 kali systemd[691]: Listening on GnuPG cryptographic agent and passphrase cache (access for web browsers).
Jan 20 00:16:07 kali systemd[691]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Jan 20 00:16:07 kali systemd[691]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Jan 20 00:16:07 kali systemd[691]: Listening on GnuPG cryptographic agent and passphrase cache.
Jan 20 00:16:07 kali systemd[691]: Listening on Sound System.
Jan 20 00:16:07 kali systemd[691]: Listening on D-Bus User Message Bus Socket.
Jan 20 00:16:07 kali systemd[691]: Reached target Sockets.
```

Right Ctrl

Oracle VM VirtualB... Balance for z2020051 Kali-Linux-2020.3-a...

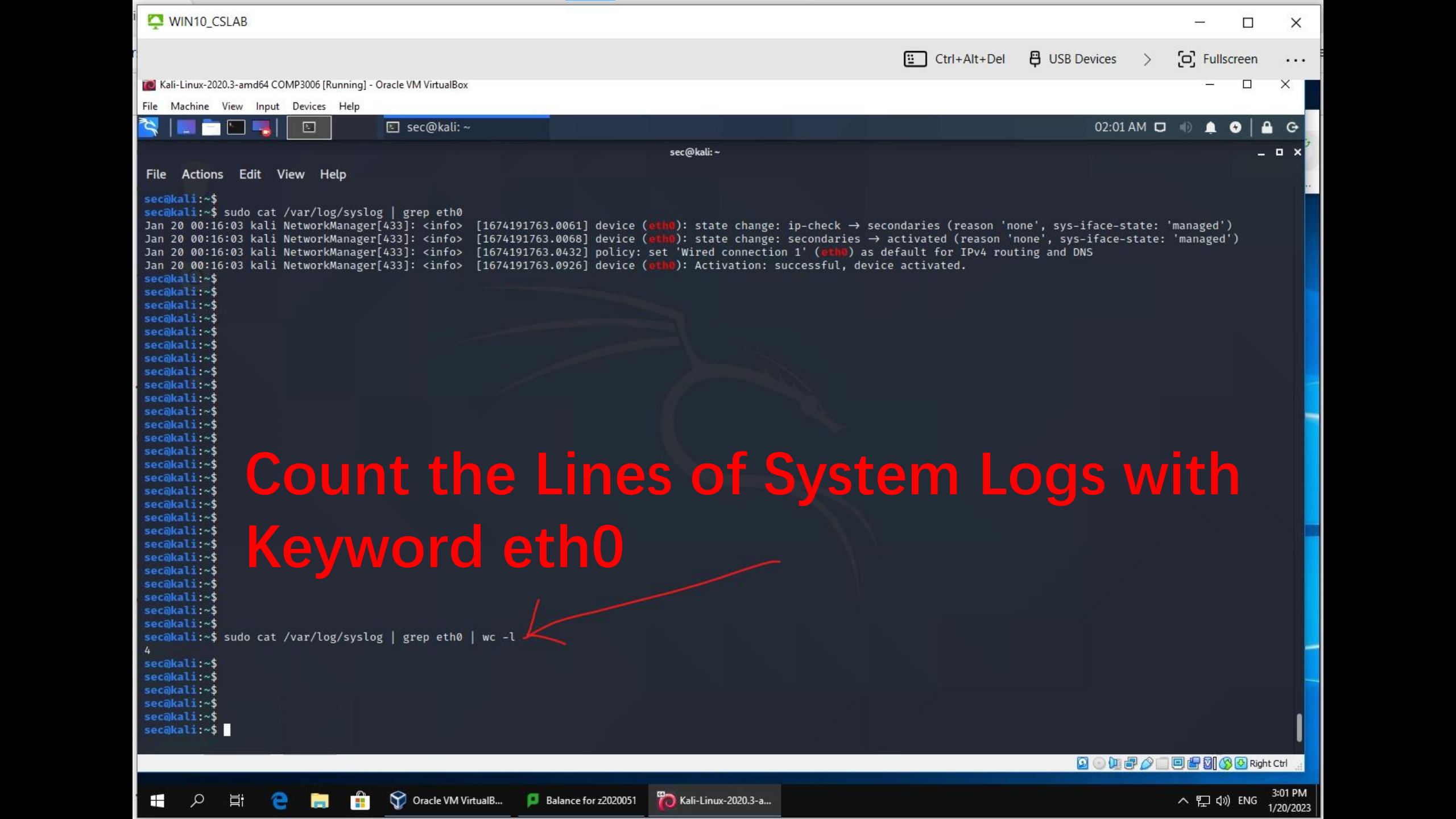
ENG 2:44 PM 1/20/2023

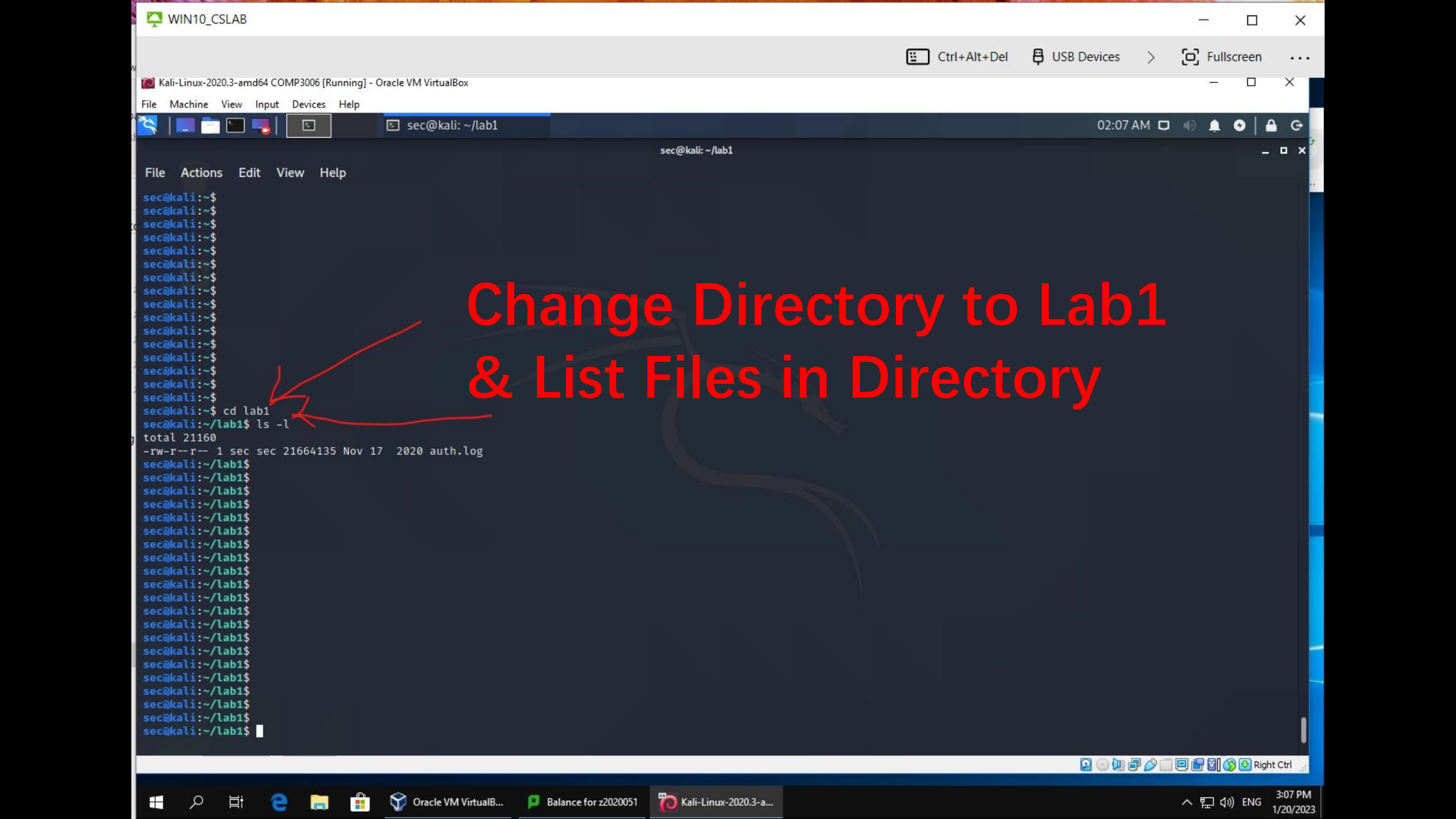

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~
01:57 AM
sec@kali: ~
File Actions Edit View Help
sec@kali:~$ sudo cat /var/log/syslog | grep eth0
Jan 20 00:16:03 kali NetworkManager[433]: <info> [1674191763.0061] device (eth0): state change: ip-check → secondaries (reason 'none', sys-iface-state: 'managed')
Jan 20 00:16:03 kali NetworkManager[433]: <info> [1674191763.0068] device (eth0): state change: secondaries → activated (reason 'none', sys-iface-state: 'managed')
Jan 20 00:16:03 kali NetworkManager[433]: <info> [1674191763.0432] policy: set 'Wired connection 1' (eth0) as default for IPv4 routing and DNS
Jan 20 00:16:03 kali NetworkManager[433]: <info> [1674191763.0926] device (eth0): Activation: successful, device activated.
Select lines of system logs with keyword “eth0”.
Note: You may need to wait for a few minutes
until the ethernet adapters are launched
and the system logs are generated
before you can use the “grep eth0” command.
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
2:57 PM
1/20/2023

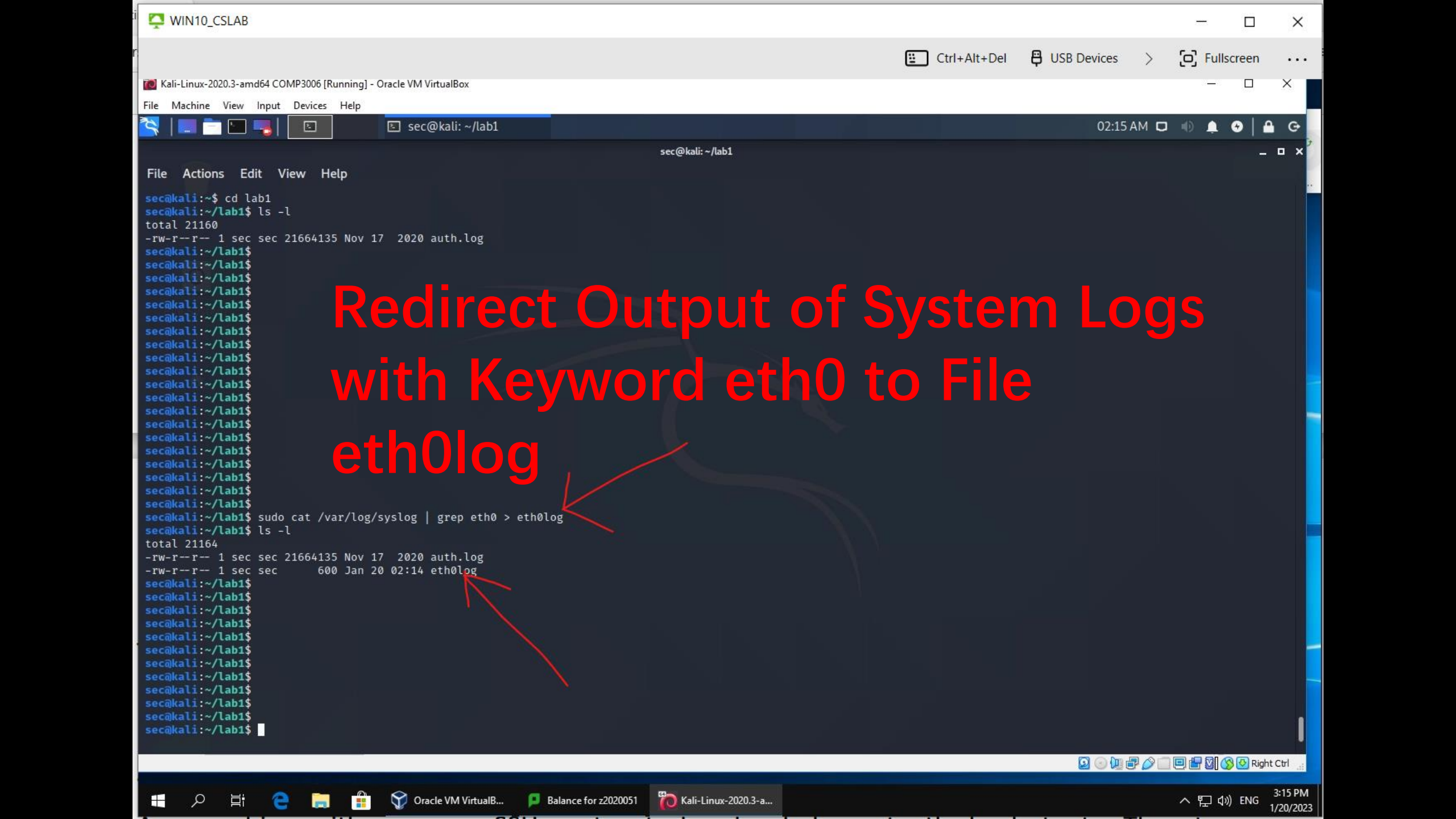
Note: If you receive this message, it is because the file is binary, and the “grep” command cannot be used directly.

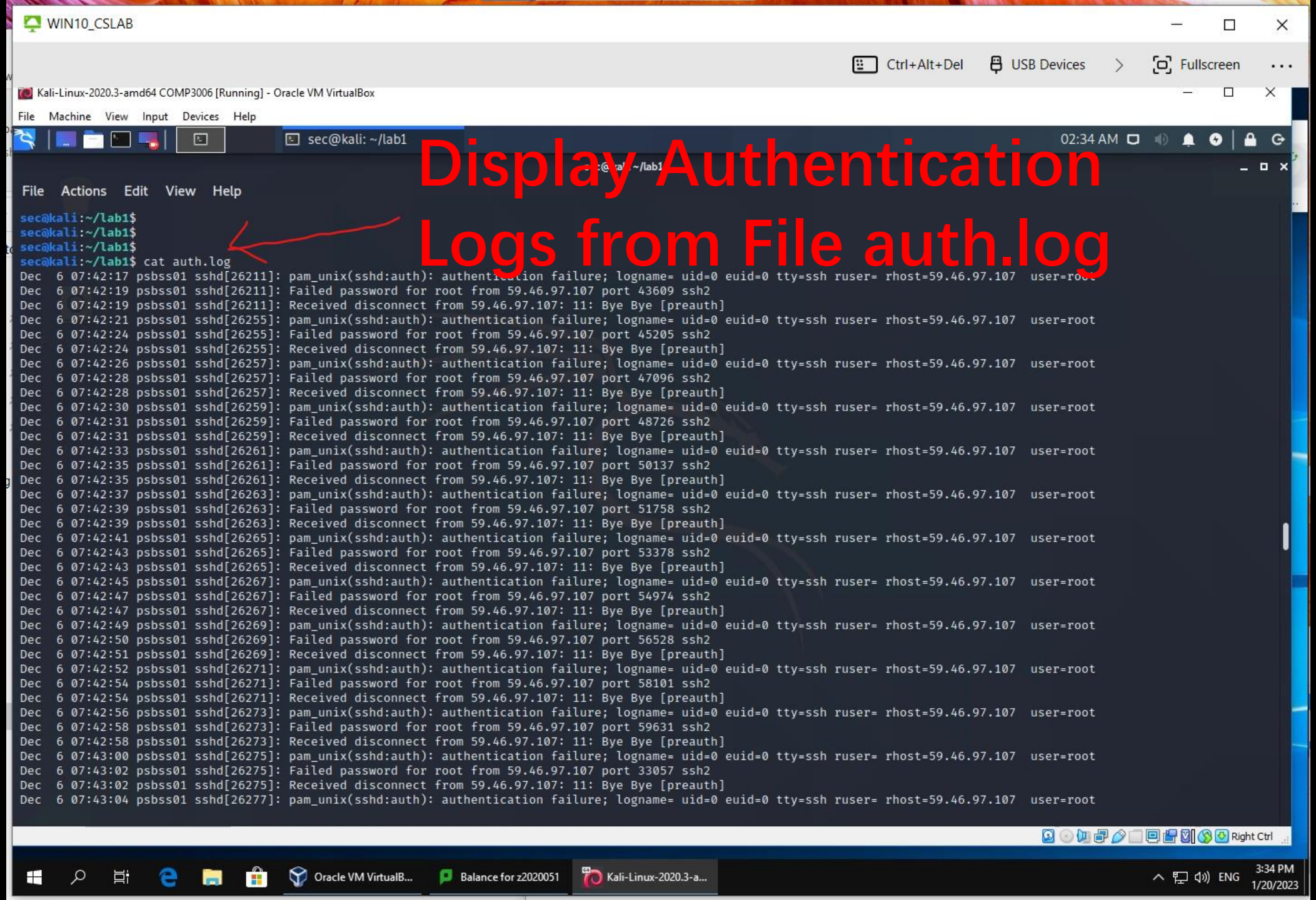
```
sec@kali:~$ sudo cat /var/log/syslog | grep eth0
Binary file (standard input) matches
sec@kali:~$ sudo cat /var/log/syslog | grep eth0
Binary file (standard input) matches
sec@kali:~$ sudo cat /var/log/syslog | grep -a eth0
Jan 25 08:46:09 kali kernel: [    6.728539] e1000 0000:00:03.0 eth0: (PCI:33MHz:32-bit) 08:00:27:5c:65:26
Jan 25 08:46:09 kali kernel: [    6.728547] e1000 0000:00:03.0 eth0: Intel(R) PRO/1000 Network Connection
Jan 25 08:46:12 kali NetworkManager[429]: <info>  [1706190372.8377] manager: (eth0): new Ethernet device (/org/freedesktop/NetworkManager/Devices/2)
Jan 25 08:46:12 kali NetworkManager[429]: <info>  [1706190372.8555] device (eth0): state change: unmanaged → unavailable (reason 'managed', sys-iface-state: 'external')
Jan 25 08:46:12 kali kernel: [   18.110773] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
Jan 25 08:46:12 kali kernel: [   18.122863] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Jan 25 08:46:12 kali NetworkManager[429]: <info>  [1706190372.8975] device (eth0): carrier: link connected
Jan 25 08:46:12 kali NetworkManager[429]: <info>  [1706190372.9505] device (eth0): state change: unavailable → disconnected (reason 'none', sys-iface-state: 'managed')
Jan 25 08:46:12 kali NetworkManager[429]: <info>  [1706190372.9926] device (eth0): Activation: starting connection 'Wired connection 1' (50e6650d-3140-4ab3-8a31-09eb50f840d2)
Jan 25 08:46:12 kali NetworkManager[429]: <info>  [1706190372.9938] device (eth0): state change: disconnected → prepare (reason 'none', sys-iface-state: 'managed')
Jan 25 08:46:12 kali NetworkManager[429]: <info>  [1706190372.9995] device (eth0): state change: prepare → config (reason 'none', sys-iface-state: 'managed')
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0094] device (eth0): state change: config → ip-config (reason 'none', sys-iface-state: 'managed')
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0120] dhcp4 (eth0): activation: beginning transaction (timeout in 45 seconds)
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0713] dhcp4 (eth0): option dhcp_lease_time      ⇒ '86400'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0714] dhcp4 (eth0): option domain_name         ⇒ 'nottingham.edu.cn'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0714] dhcp4 (eth0): option domain_name_servers ⇒ '10.178.2.128 10.2.1.6'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0714] dhcp4 (eth0): option expiry             ⇒ '1706276773'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0714] dhcp4 (eth0): option ip_address         ⇒ '10.0.2.15'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0715] dhcp4 (eth0): option next_server       ⇒ '10.0.2.4'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0715] dhcp4 (eth0): option requested_broadcast_address ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0716] dhcp4 (eth0): option requested_domain_name ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0716] dhcp4 (eth0): option requested_domain_name_servers ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0716] dhcp4 (eth0): option requested_domain_search ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0717] dhcp4 (eth0): option requested_host_name  ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0717] dhcp4 (eth0): option requested_interface_mtu ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0717] dhcp4 (eth0): option requested_ms_classless_static_routes ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0717] dhcp4 (eth0): option requested_nis_domain ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0718] dhcp4 (eth0): option requested_nis_servers ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0718] dhcp4 (eth0): option requested_ntp_servers ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0718] dhcp4 (eth0): option requested_rfc3442_classless_static_routes ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0718] dhcp4 (eth0): option requested_root_path  ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0719] dhcp4 (eth0): option requested_routers    ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0719] dhcp4 (eth0): option requested_static_routes ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0719] dhcp4 (eth0): option requested_subnet_mask ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0720] dhcp4 (eth0): option requested_time_offset ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0721] dhcp4 (eth0): option requested_wpad       ⇒ '1'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0721] dhcp4 (eth0): option routers             ⇒ '10.0.2.2'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0721] dhcp4 (eth0): option subnet_mask        ⇒ '255.255.255.0'
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0721] dhcp4 (eth0): state changed unknown → bound
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.0781] device (eth0): state change: ip-config → ip-check (reason 'none', sys-iface-state: 'managed')
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.1002] device (eth0): state change: ip-check → secondaries (reason 'none', sys-iface-state: 'managed')
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.1021] device (eth0): state change: secondaries → activated (reason 'none', sys-iface-state: 'managed')
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.1139] policy: set 'Wired connection 1' (eth0) as default for IPv4 routing and DNS
Jan 25 08:46:13 kali NetworkManager[429]: <info>  [1706190373.1350] device (eth0): Activation: successful, device activated.
```

Add *-a* option to the “grep” command, which will allow it to work on binary files.

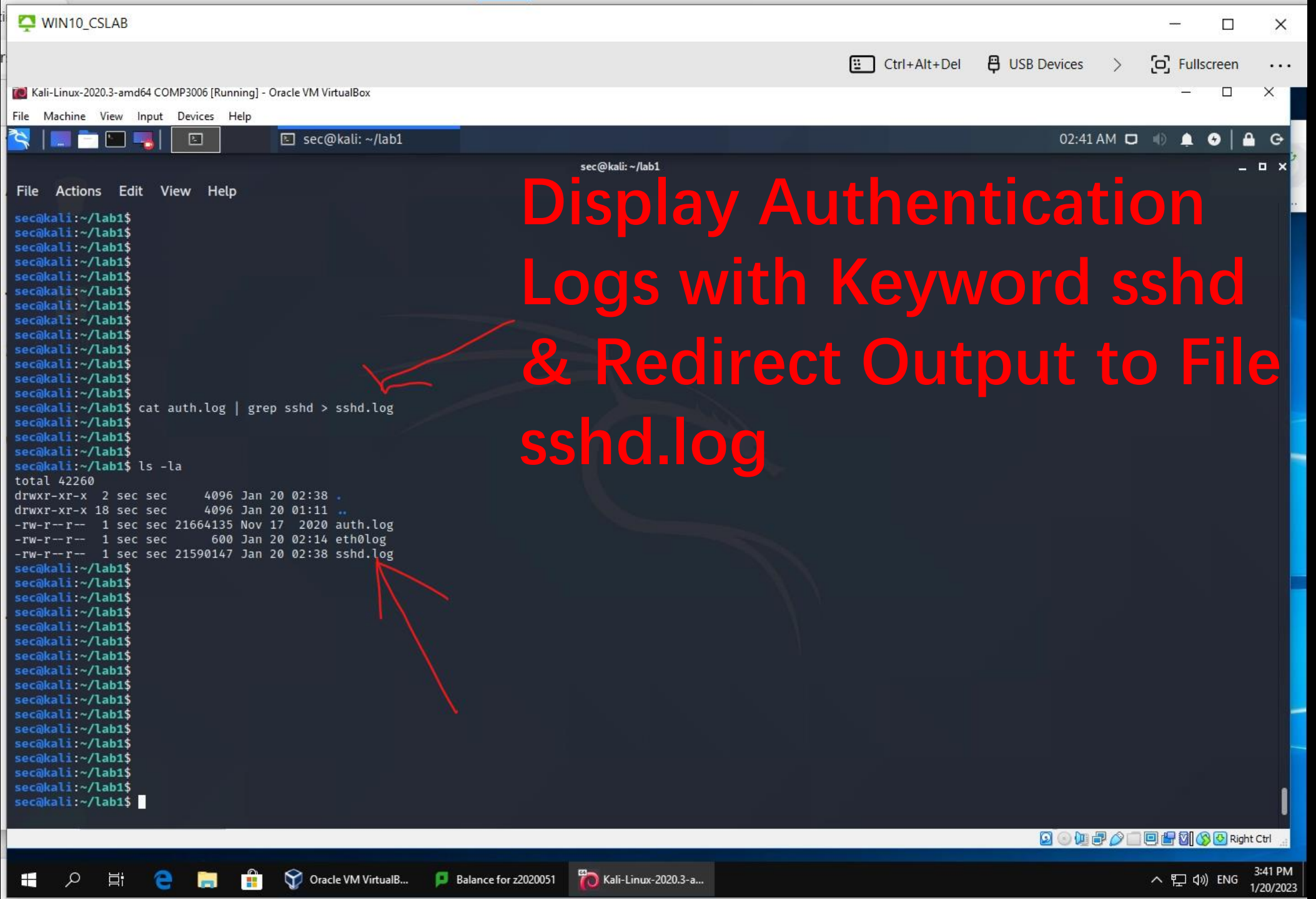

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~
02:01 AM
sec@kali: ~
File Actions Edit View Help
sec@kali:~$
sec@kali:~$ sudo cat /var/log/syslog | grep eth0
Jan 20 00:16:03 kali NetworkManager[433]: <info> [1674191763.0061] device (eth0): state change: ip-check → secondaries (reason 'none', sys-iface-state: 'managed')
Jan 20 00:16:03 kali NetworkManager[433]: <info> [1674191763.0068] device (eth0): state change: secondaries → activated (reason 'none', sys-iface-state: 'managed')
Jan 20 00:16:03 kali NetworkManager[433]: <info> [1674191763.0432] policy: set 'Wired connection 1' (eth0) as default for IPv4 routing and DNS
Jan 20 00:16:03 kali NetworkManager[433]: <info> [1674191763.0926] device (eth0): Activation: successful, device activated.
Count the Lines of System Logs with Keyword eth0
sec@kali:~$ sudo cat /var/log/syslog | grep eth0 | wc -l
4
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
3:01 PM
1/20/2023

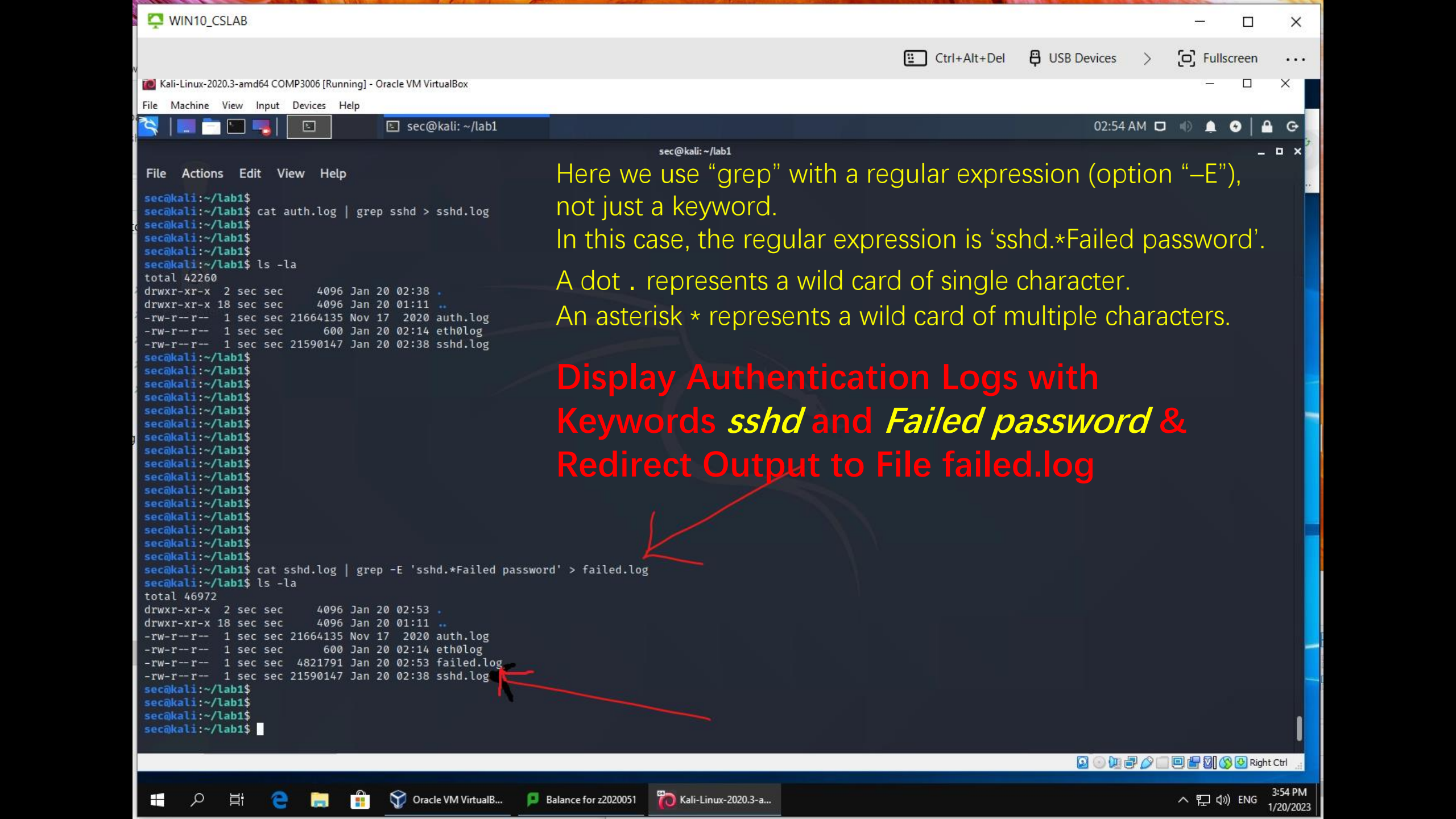

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
02:07 AM
sec@kali: ~/lab1
File Actions Edit View Help
sec@kali:~$ cd lab1
sec@kali:~/lab1$ ls -l
total 21160
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
Change Directory to Lab1
& List Files in Directory
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
3:07 PM
1/20/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
02:15 AM
sec@kali: ~/lab1
File Actions Edit View Help
sec@kali:~$ cd lab1
sec@kali:~/lab1$ ls -l
total 21160
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
sec@kali:~/lab1$ sudo cat /var/log/syslog | grep eth0 > eth0log
sec@kali:~/lab1$ ls -l
total 21164
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
-rw-r--r-- 1 sec sec 600 Jan 20 02:14 eth0log
Redirect Output of System Logs with Keyword eth0 to File eth0log
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
3:15 PM
1/20/2023



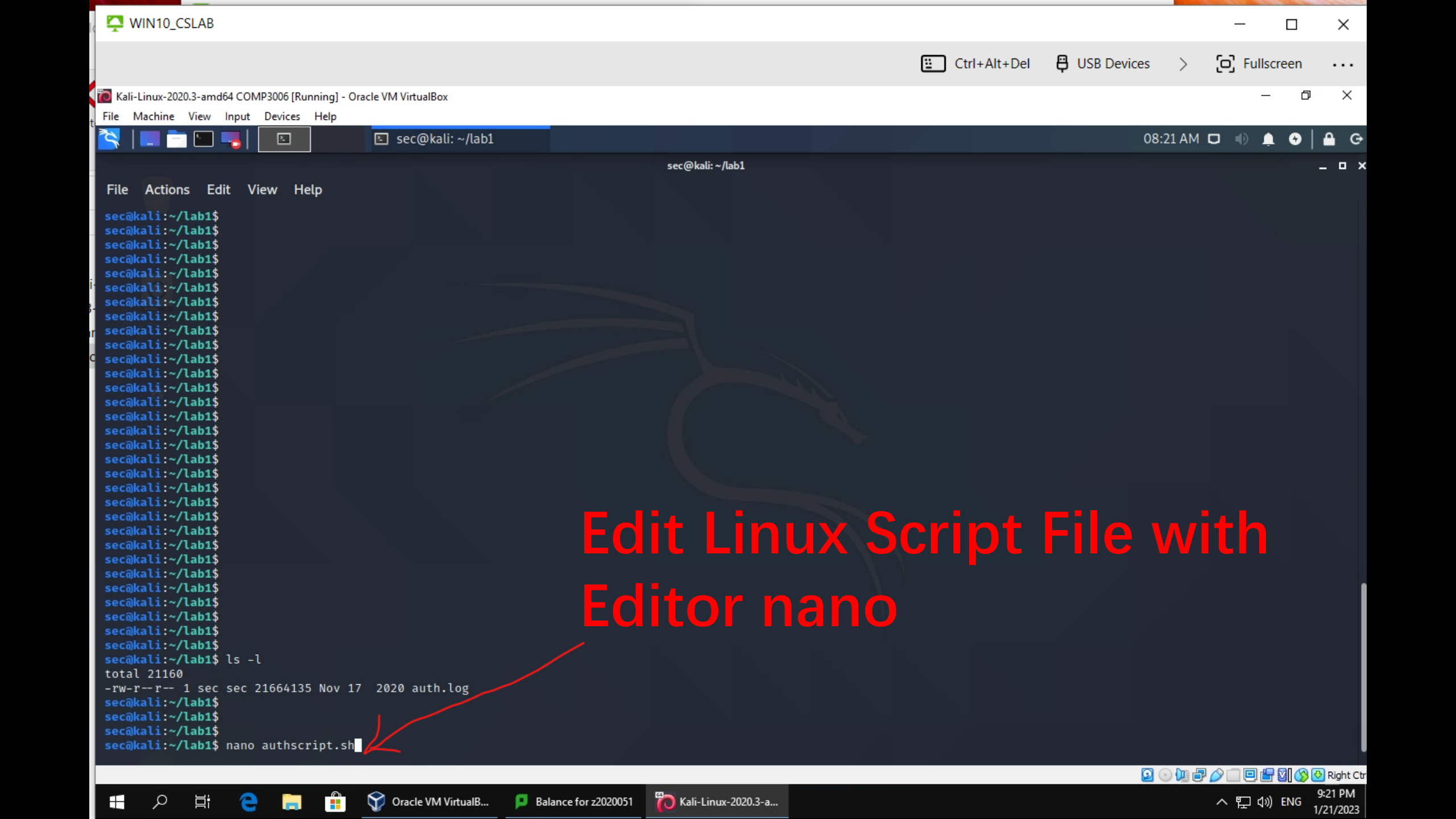
Display Authentication Logs from File auth.log

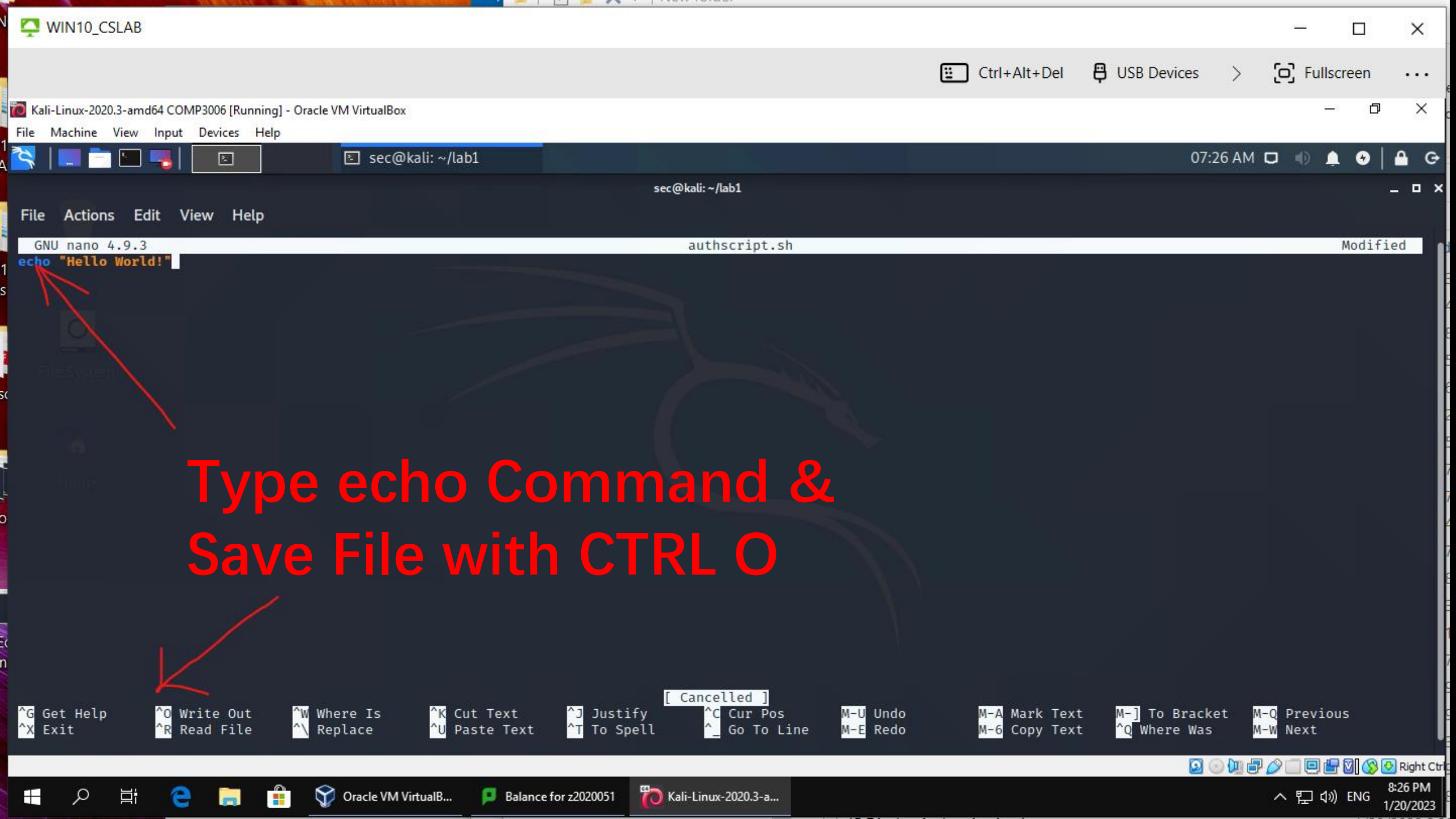

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
02:41 AM
sec@kali: ~/lab1
File Actions Edit View Help
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ cat auth.log | grep sshd > sshd.log
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ ls -la
total 42260
drwxr-xr-x 2 sec sec 4096 Jan 20 02:38 .
drwxr-xr-x 18 sec sec 4096 Jan 20 01:11 ..
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
-rw-r--r-- 1 sec sec 600 Jan 20 02:14 eth0log
-rw-r--r-- 1 sec sec 21590147 Jan 20 02:38 sshd.log
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
Display Authentication Logs with Keyword sshd & Redirect Output to File sshd.log
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
3:41 PM
1/20/2023

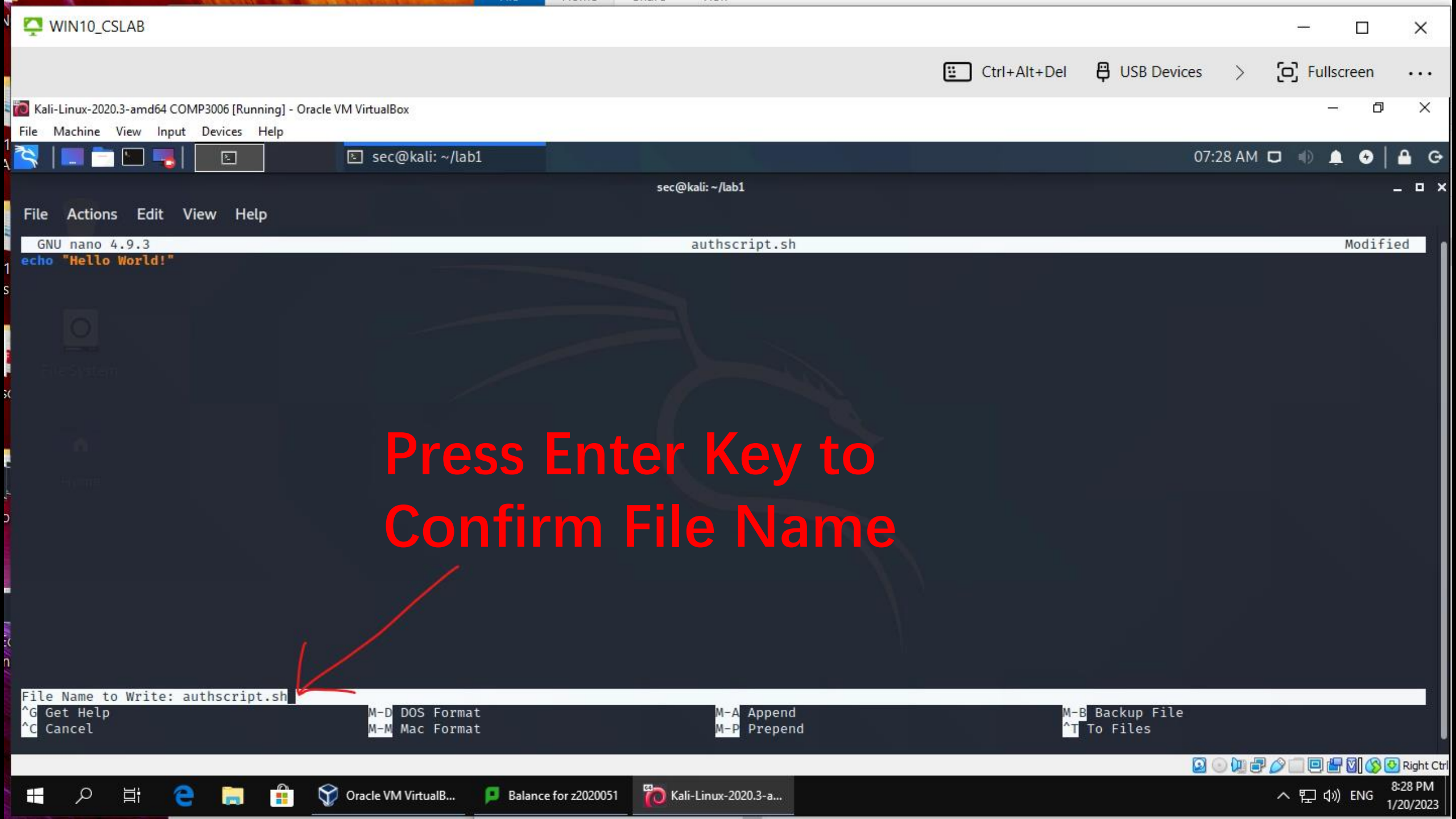

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
02:54 AM
sec@kali: ~/lab1
File Actions Edit View Help
sec@kali:~/lab1$
sec@kali:~/lab1$ cat auth.log | grep sshd > sshd.log
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ ls -la
total 42260
drwxr-xr-x 2 sec sec 4096 Jan 20 02:38 .
drwxr-xr-x 18 sec sec 4096 Jan 20 01:11 ..
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
-rw-r--r-- 1 sec sec 600 Jan 20 02:14 eth0log
-rw-r--r-- 1 sec sec 21590147 Jan 20 02:38 sshd.log
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ cat sshd.log | grep -E 'sshd.*Failed password' > failed.log
sec@kali:~/lab1$ ls -la
total 46972
drwxr-xr-x 2 sec sec 4096 Jan 20 02:53 .
drwxr-xr-x 18 sec sec 4096 Jan 20 01:11 ..
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
-rw-r--r-- 1 sec sec 600 Jan 20 02:14 eth0log
-rw-r--r-- 1 sec sec 4821791 Jan 20 02:53 failed.log
-rw-r--r-- 1 sec sec 21590147 Jan 20 02:38 sshd.log
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
Here we use “grep” with a regular expression (option “–E”), not just a keyword.
In this case, the regular expression is ‘sshd.*Failed password’.
A dot . represents a wild card of single character.
An asterisk * represents a wild card of multiple characters.
Display Authentication Logs with Keywords sshd and Failed password & Redirect Output to File failed.log
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
3:54 PM
1/20/2023

Editing Linux Script File (Program File)

- In the next few slides, you will learn how to edit a Linux script file (program file), which contains a sequence of Linux commands.
- You will use the command called “nano” to launch the editor for editing a Linux script file.
- The name of a Linux script file should end with an extension “.sh”.


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
08:21 AM
sec@kali: ~/lab1
File Actions Edit View Help
sec@kali:~/lab1$ ls -l
total 21160
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
sec@kali:~/lab1$ nano authscript.sh
Edit Linux Script File with Editor nano
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
9:21 PM
1/21/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
07:26 AM
sec@kali: ~/lab1
File Actions Edit View Help
GNU nano 4.9.3 authscript.sh Modified
echo "Hello World!"
Type echo Command &
Save File with CTRL O
[Cancelled]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text M-] To Bracket M-Q Previous
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text ^Q Where Was M-W Next
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
8:26 PM
1/20/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
07:28 AM
sec@kali: ~/lab1
File Actions Edit View Help
GNU nano 4.9.3 authscript.sh Modified
echo "Hello World!"
Press Enter Key to
Confirm File Name
File Name to Write: authscript.sh
^G Get Help M-D DOS Format M-A Append M-B Backup File
^C Cancel M-M Mac Format M-P Prepend ^T To Files
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
8:28 PM
1/20/2023

WIN10_CSLAB

Ctrl+Alt+Del | USB Devices | Fullscreen

Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~/lab1 07:30 AM

sec@kali: ~/lab1

File Actions Edit View Help

```
 GNU nano 4.9.3                                    authscript.sh
echo "Hello World!"
```

Exit Editor with CTRL X

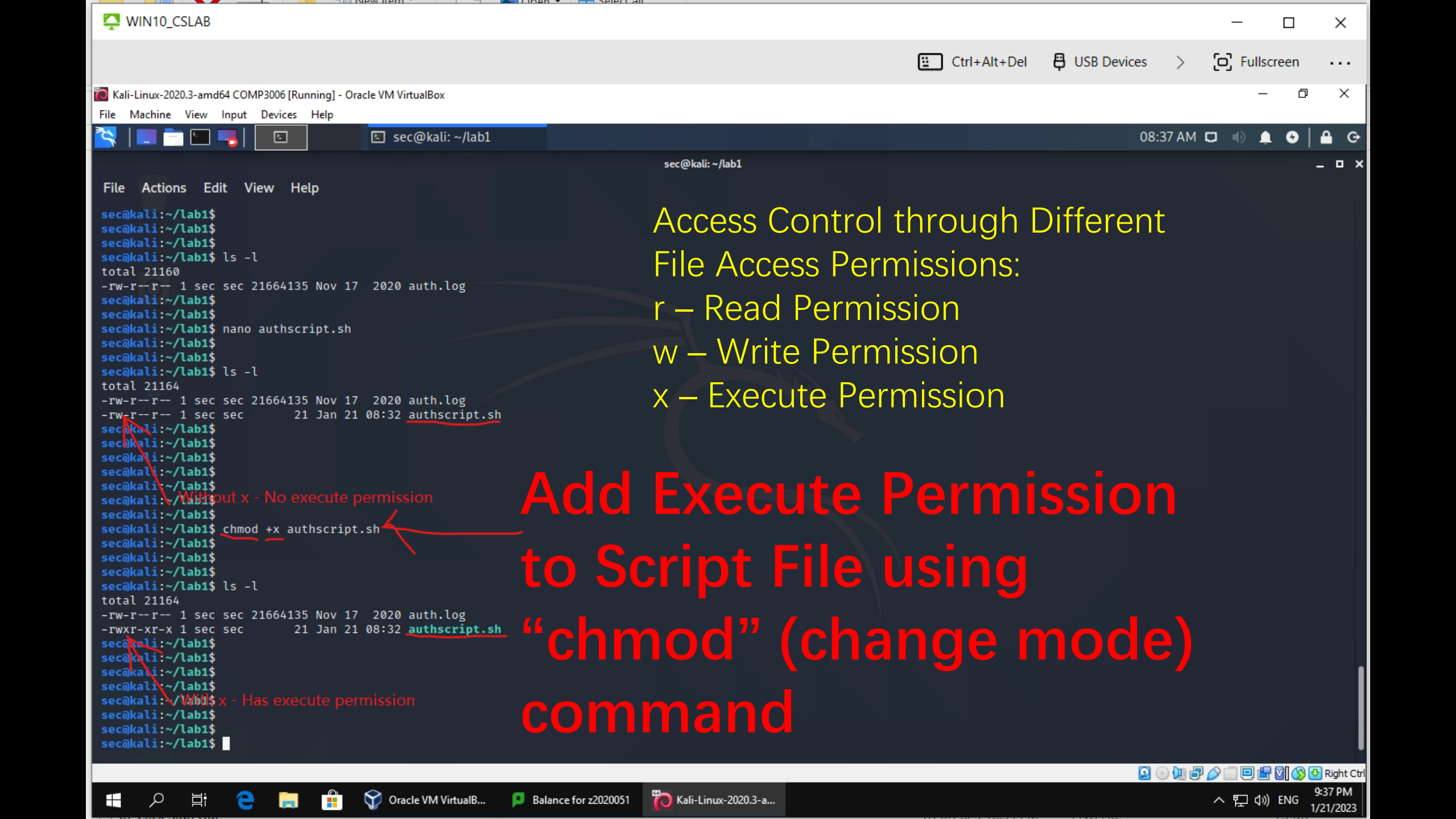
[Wrote 1 line]

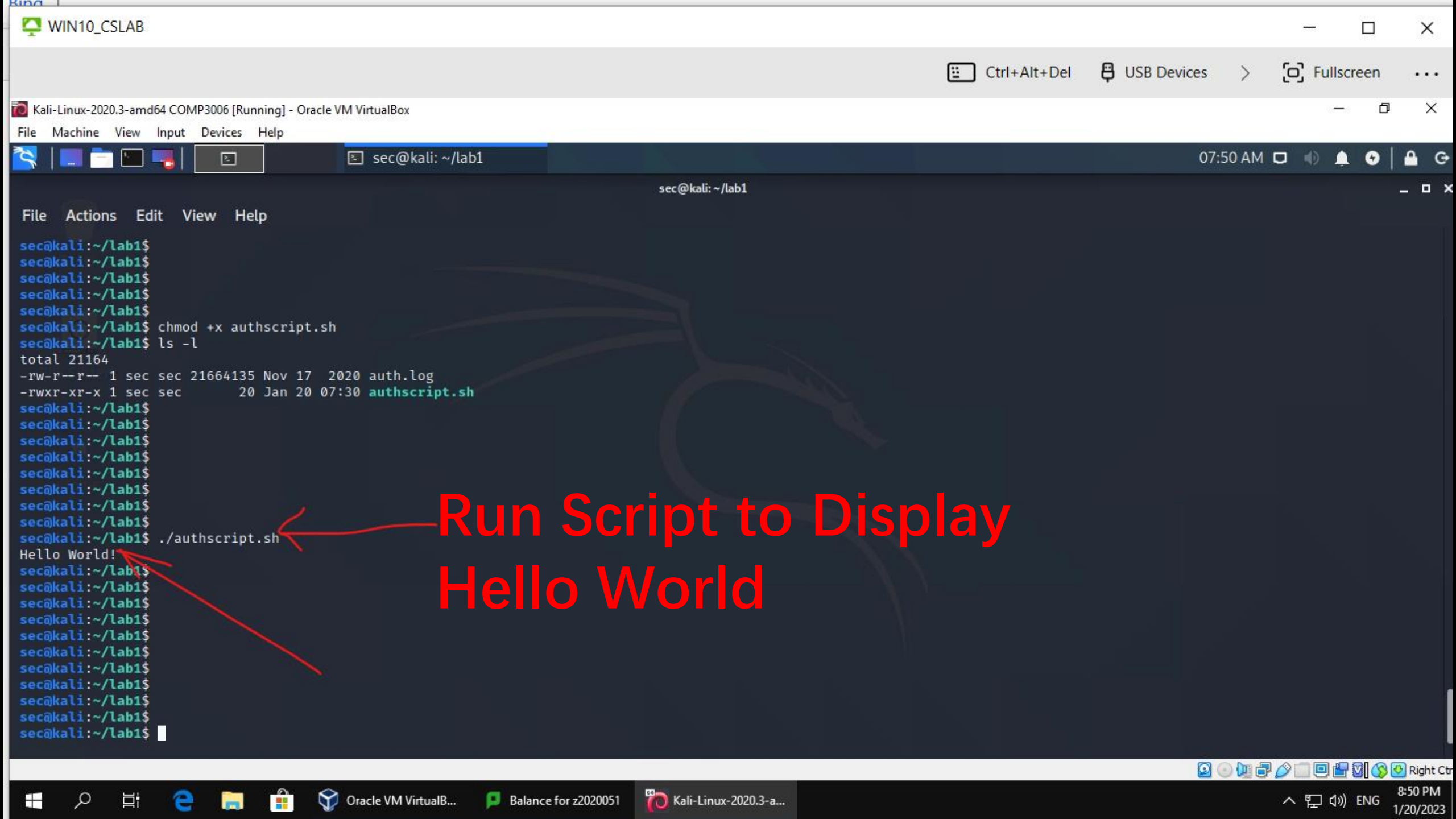
```
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo   M-A Mark Text   M-] To Bracket   M-Q Previous
^X Exit       ^R Read File   ^\ Replace    ^U Paste Text ^T To Spell  ^_ Go To Line M-E Redo   M-6 Copy Text   ^Q Where Was     M-W Next
```

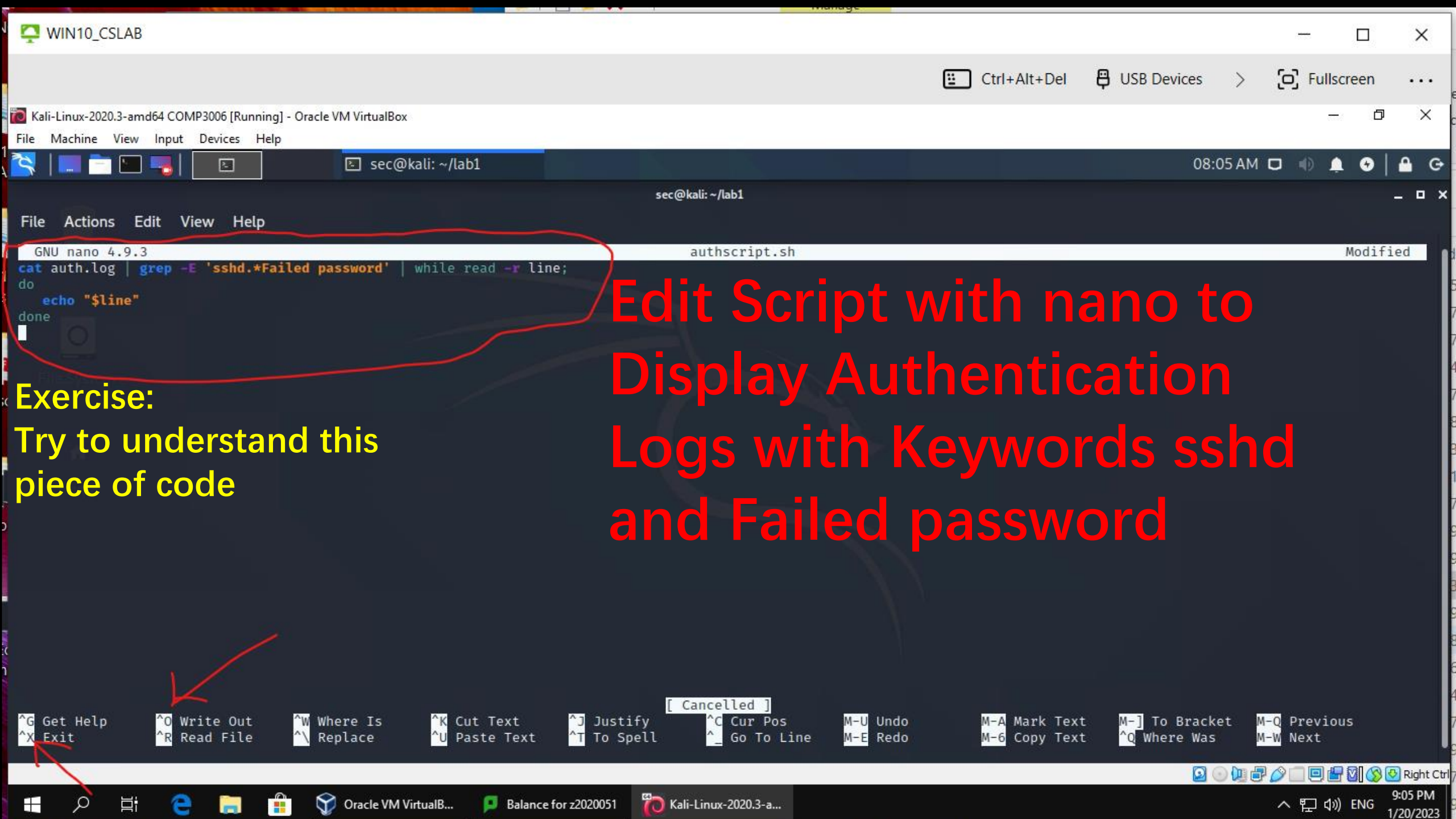
Right Ctrl

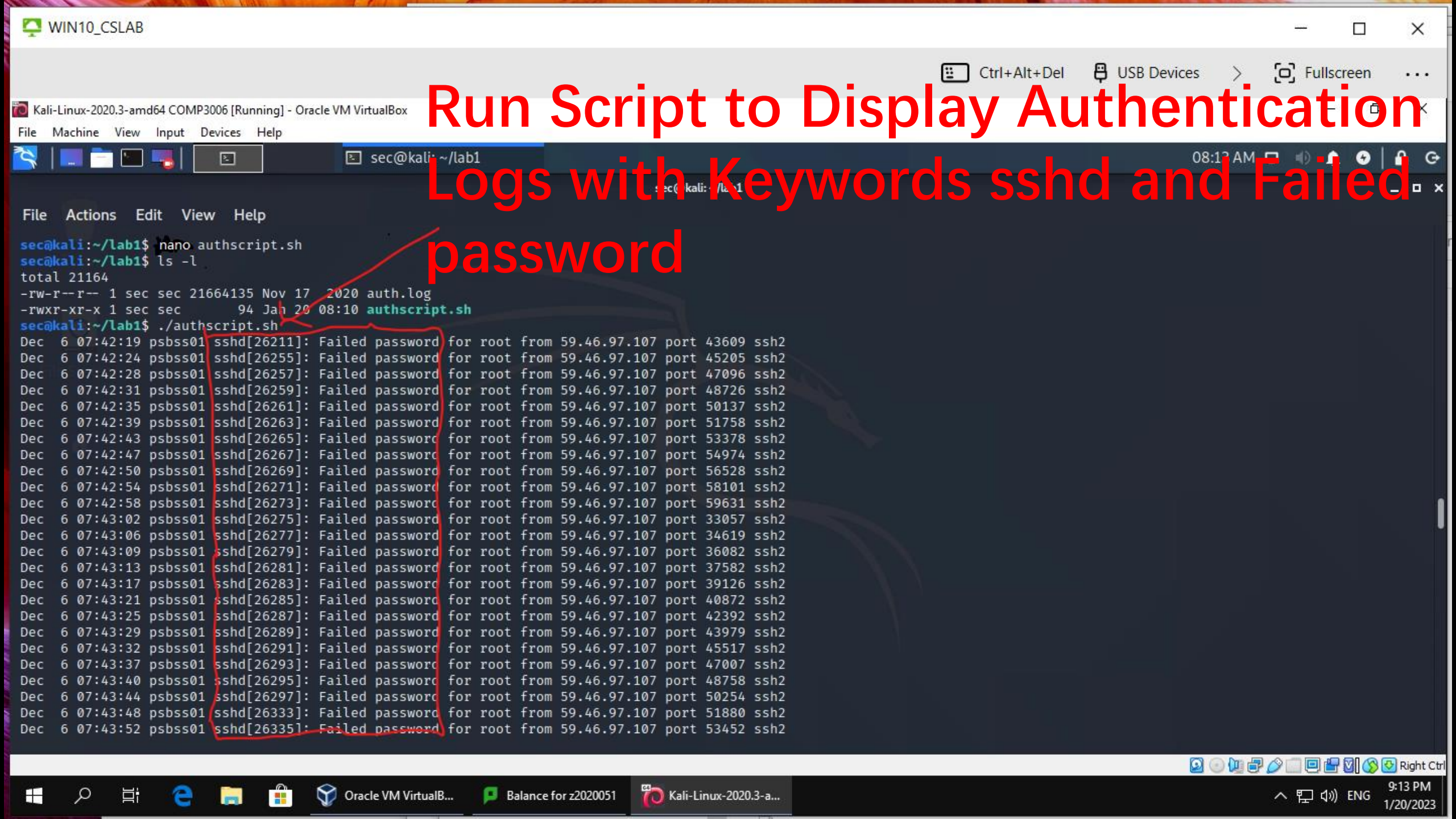
Oracle VM VirtualB... | Balance for z2020051 | Kali-Linux-2020.3-a...

ENG 8:30 PM 1/20/2023

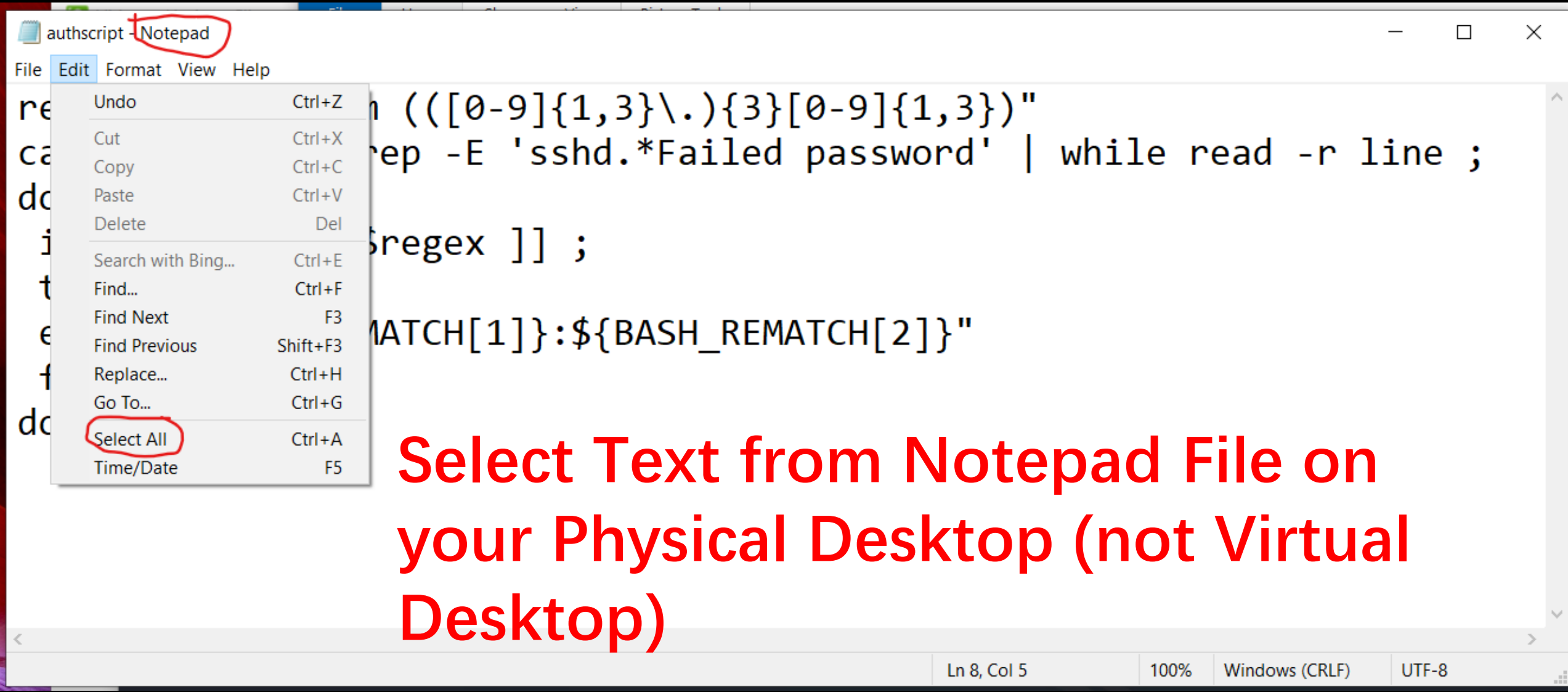

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
08:37 AM
sec@kali: ~/lab1
File Actions Edit View Help
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ ls -l
total 21160
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ nano authscript.sh
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ ls -l
total 21164
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
-rw-r--r-- 1 sec sec 21 Jan 21 08:32 authscript.sh
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ chmod +x authscript.sh
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ ls -l
total 21164
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
-rwxr-xr-x 1 sec sec 21 Jan 21 08:32 authscript.sh
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
Without x - No execute permission
With x - Has execute permission
Access Control through Different File Access Permissions:
r – Read Permission
w – Write Permission
x – Execute Permission
Add Execute Permission to Script File using “chmod” (change mode) command
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
9:37 PM
1/21/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
07:50 AM
sec@kali: ~/lab1
File Actions Edit View Help
sec@kali:~/lab1$ chmod +x authscript.sh
sec@kali:~/lab1$ ls -l
total 21164
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
-rwxr-xr-x 1 sec sec 20 Jan 20 07:30 authscript.sh
sec@kali:~/lab1$ ./authscript.sh
Hello World!
Run Script to Display
Hello World
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
8:50 PM
1/20/2023

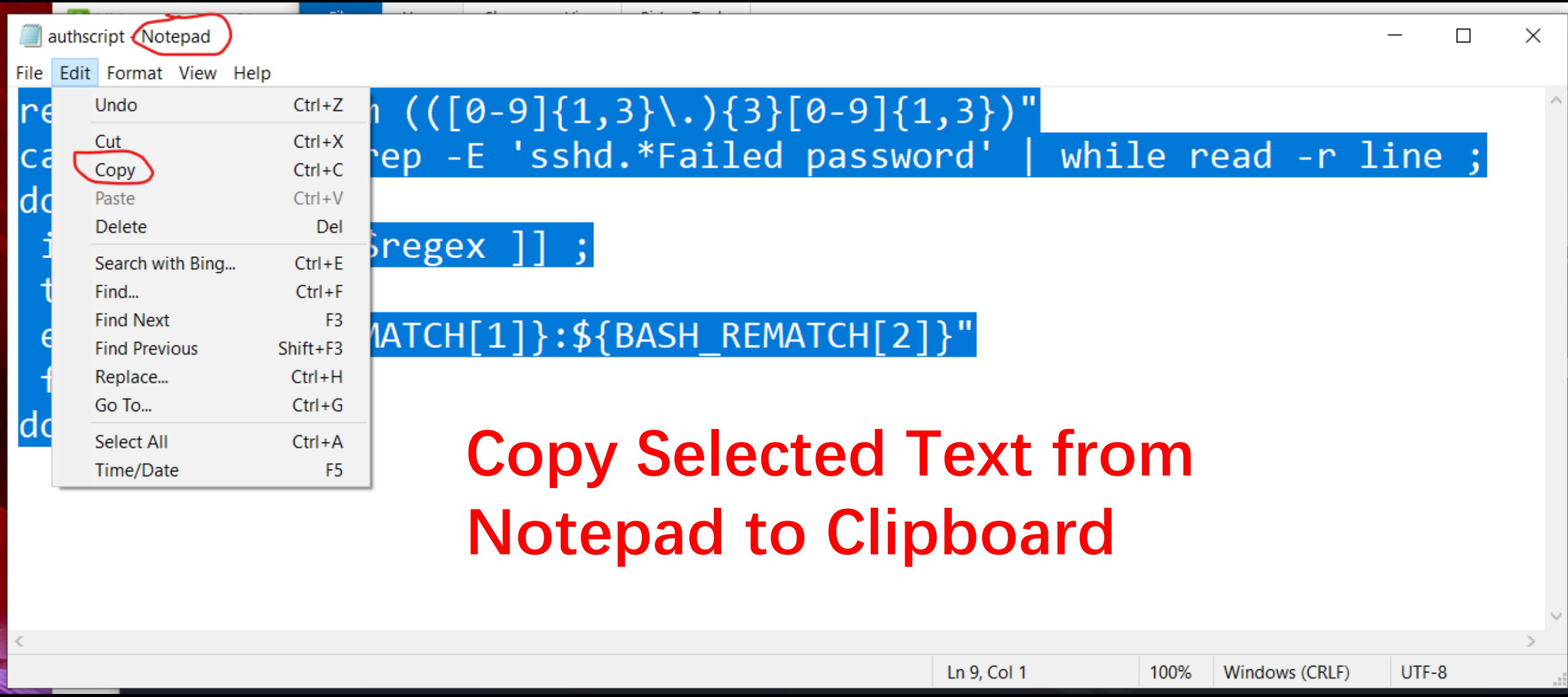

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
08:05 AM
sec@kali: ~/lab1
File Actions Edit View Help
GNU nano 4.9.3 authscript.sh Modified
cat auth.log | grep -E 'sshd.*Failed password' | while read -r line;
do
echo "$line"
done
Edit Script with nano to Display Authentication Logs with Keywords sshd and Failed password
Exercise:
Try to understand this piece of code
[Cancelled]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text M-] To Bracket M-Q Previous
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text ^Q Where Was M-W Next
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
9:05 PM
1/20/2023

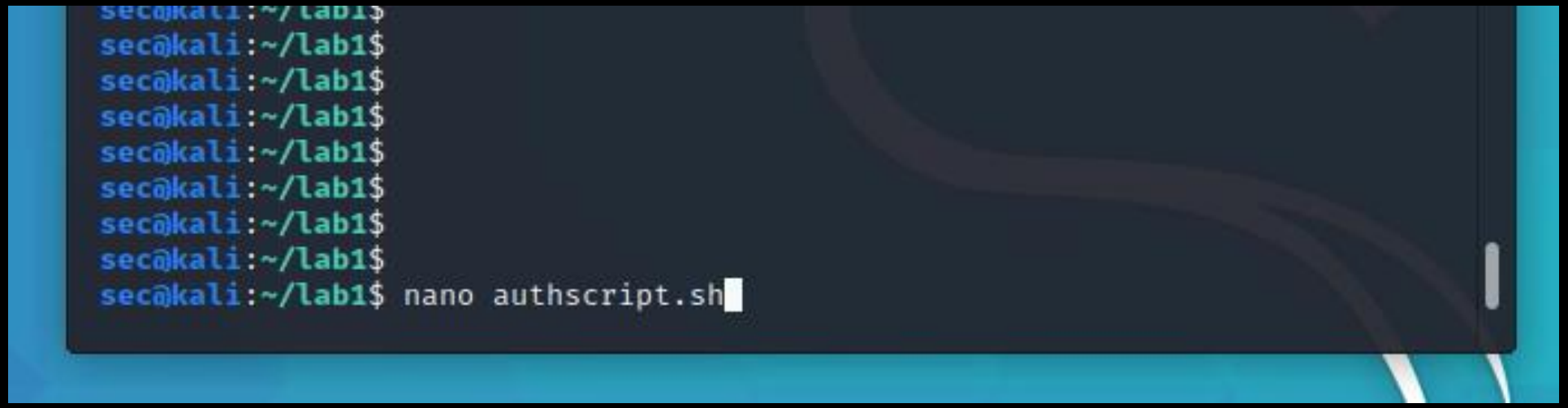


Run Script to Display Authentication Logs with Keywords sshd and Failed password

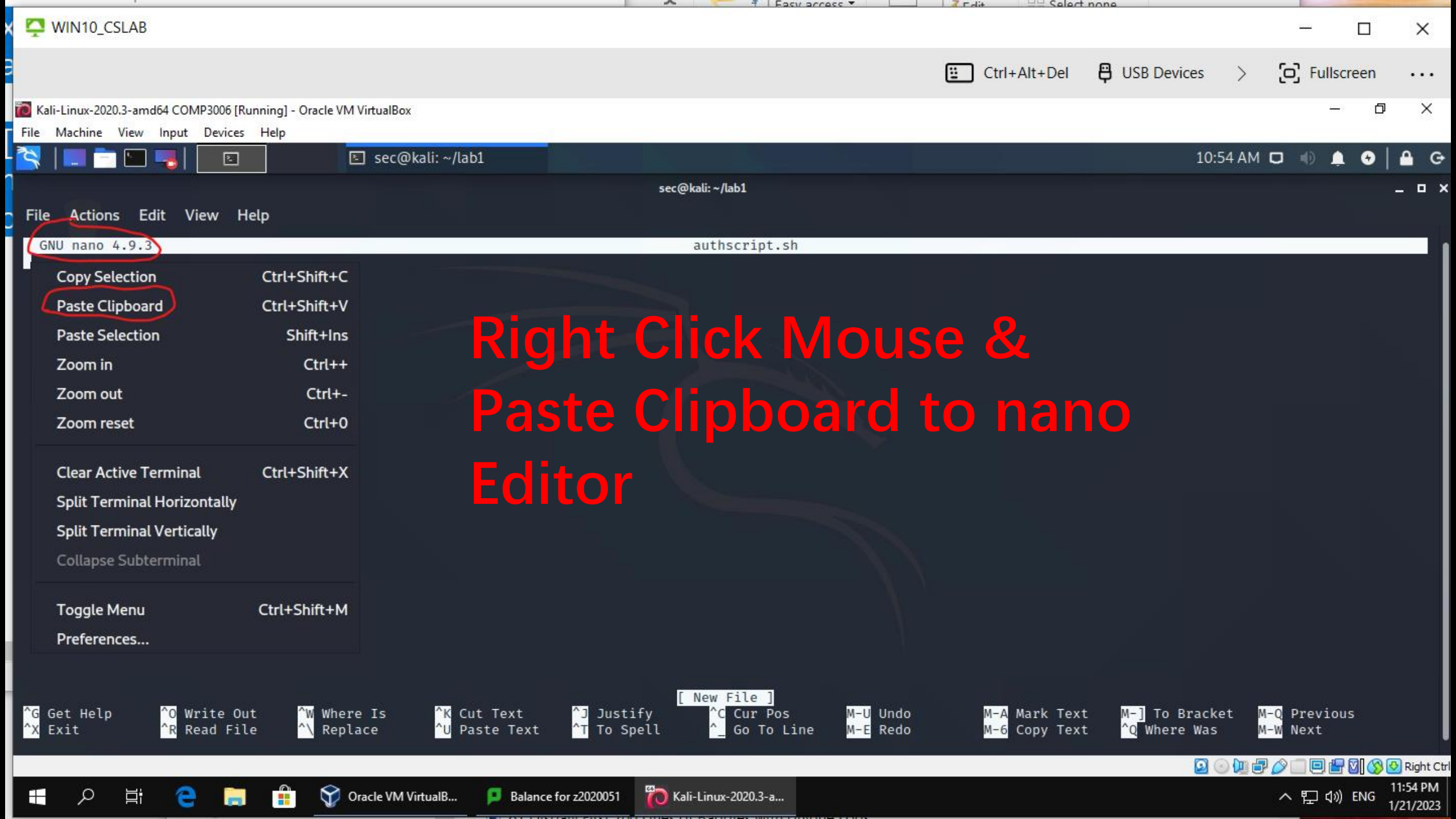


Select Text from Notepad File on your Physical Desktop (not Virtual Desktop)


authscript - Notepad
File Edit Format View Help
Undo Ctrl+Z
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Delete Del
Search with Bing... Ctrl+E
Find... Ctrl+F
Find Next F3
Find Previous Shift+F3
Replace... Ctrl+H
Go To... Ctrl+G
Select All Ctrl+A
Time/Date F5
(([0-9]{1,3}\.){3}[0-9]{1,3})"
ep -E 'sshd.*Failed password' | while read -r line ;
regex]] ;
ATCH[1]}:${BASH_REMATCH[2]}"
Copy Selected Text from
Notepad to Clipboard
Ln 9, Col 1
100%
Windows (CRLF)
UTF-8



Edit Linux Script File with Editor nano


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
10:54 AM
sec@kali: ~/lab1
File Actions Edit View Help
GNU nano 4.9.3 authscript.sh
Copy Selection Ctrl+Shift+C
Paste Clipboard Ctrl+Shift+V
Paste Selection Shift+Ins
Zoom in Ctrl++
Zoom out Ctrl+-
Zoom reset Ctrl+0
Clear Active Terminal Ctrl+Shift+X
Split Terminal Horizontally
Split Terminal Vertically
Collapse Subterminal
Toggle Menu Ctrl+Shift+M
Preferences...
Right Click Mouse &
Paste Clipboard to nano
Editor
[New File]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text M-] To Bracket M-Q Previous
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text ^Q Where Was M-W Next
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
11:54 PM
1/21/2023

WIN10_CSLAB

Ctrl+Alt+Del | USB Devices | Fullscreen

Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~/lab1 — 10:56 AM

sec@kali: ~/lab1

File Actions Edit View Help

GNU nano 4.9.3 — authscript.sh — Modified

```
regex="(\S+) from (([0-9]{1,3}\.){3}[0-9]{1,3})"
cat auth.log | grep -E 'sshd.*Failed password' | while read -r line ;
do
 if [[ $line =~ $regex ]] ;
 then
 echo "${BASH_REMATCH[1]}:${BASH_REMATCH[2]}"
 fi
done
```

Exercise:
Try to understand this piece of code

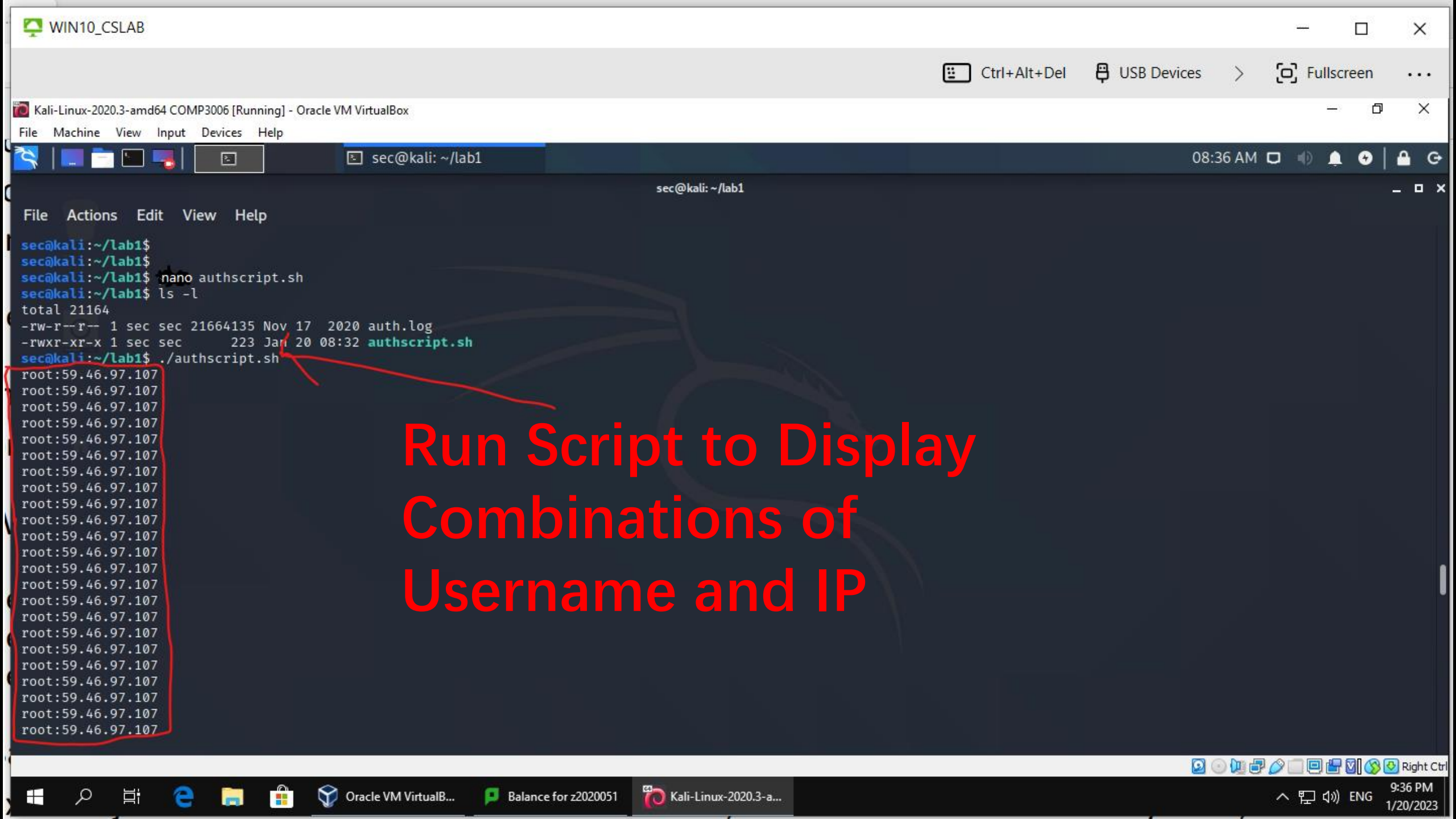
Save & Exit Script to Display Combinations of Username and IP

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text M-] To Bracket M-Q Previous
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text ^Q Where Was M-W Next

Right Ctrl

Oracle VM VirtualB... | Balance for z2020051 | Kali-Linux-2020.3-a...

ENG 11:56 PM 1/21/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
08:36 AM
sec@kali: ~/lab1
File Actions Edit View Help
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ nano authscript.sh
sec@kali:~/lab1$ ls -l
total 21164
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
-rwxr-xr-x 1 sec sec 223 Jan 20 08:32 authscript.sh
sec@kali:~/lab1$ ./authscript.sh
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
root:59.46.97.107
Run Script to Display Combinations of Username and IP
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
9:36 PM
1/20/2023

WIN10_CSLAB

Ctrl+Alt+Del | USB Devices | Fullscreen

Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~/lab1 | 08:40 AM

sec@kali: ~/lab1

File Actions Edit View Help

```
 GNU nano 4.9.3                          authscript.sh                          Modified
regex="(\S+) from (([0-9]{1,3}\.){3}[0-9]{1,3})"
cat auth.log | grep -E 'sshd.*Failed password' | while read -r line;
do
   if [[ $line =~ $regex ]];
   then
      echo "${BASH_REMATCH[1]}:${BASH_REMATCH[2]}"
   fi
done | sort | uniq
```

Exercise:
Try to understand this piece of code

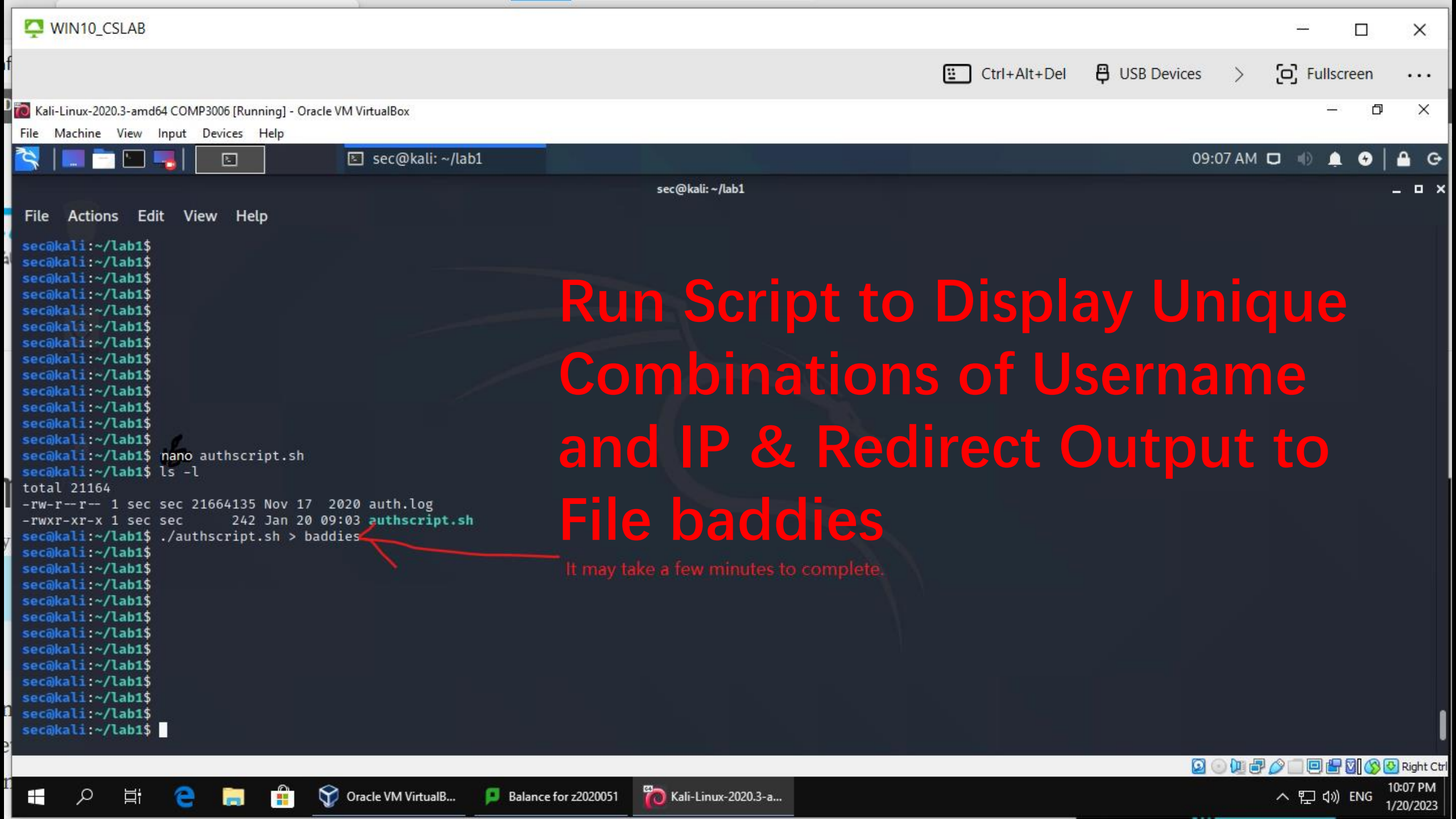
Edit Script to Display Unique Combinations of Username and IP

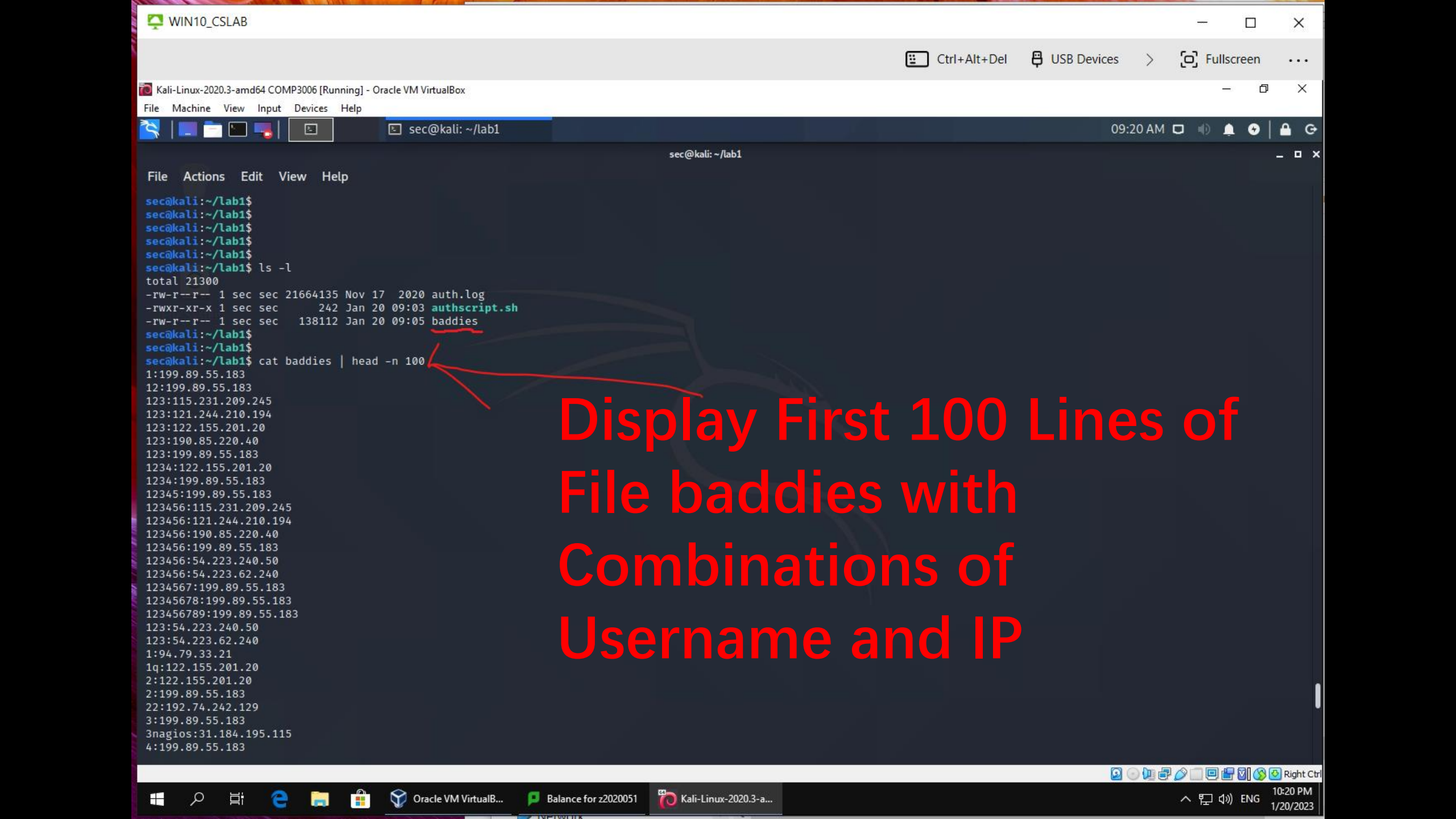
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text M-] To Bracket M-Q Previous
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text ^Q Where Was M-W Next

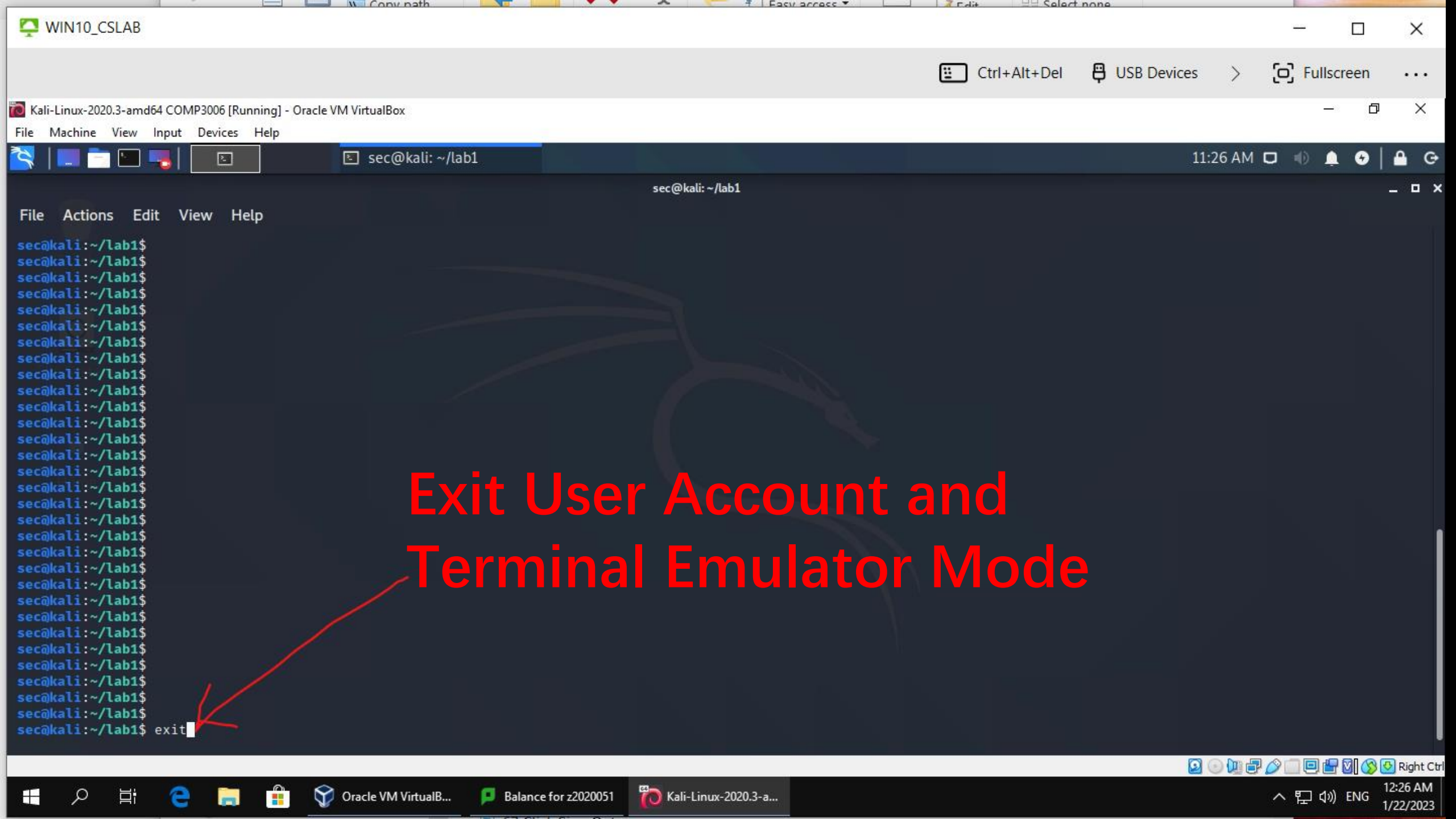
Right Ctrl

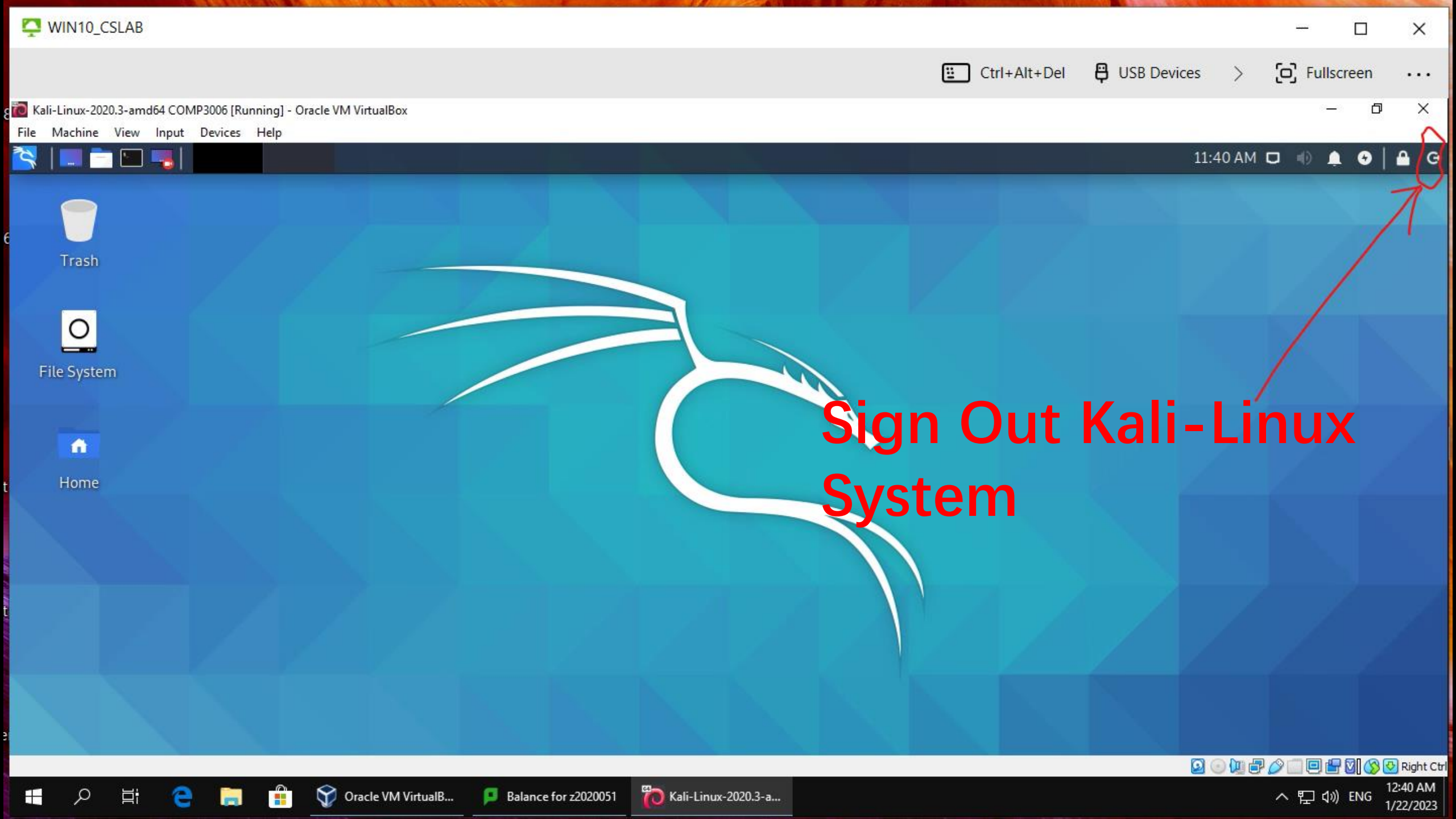
Oracle VM VirtualB... | Balance for z2020051 | Kali-Linux-2020.3-a...

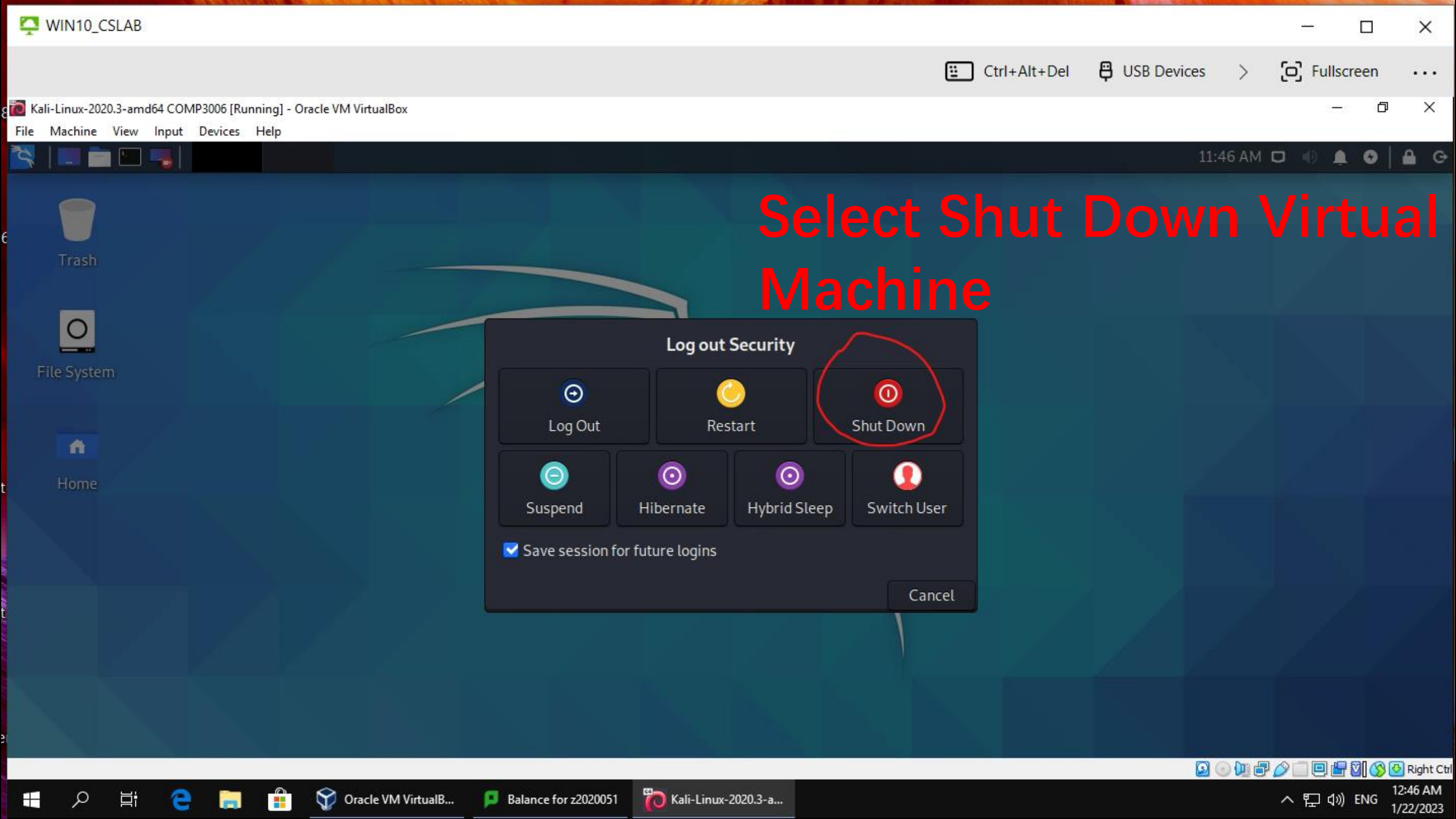
ENG 9:40 PM 1/20/2023

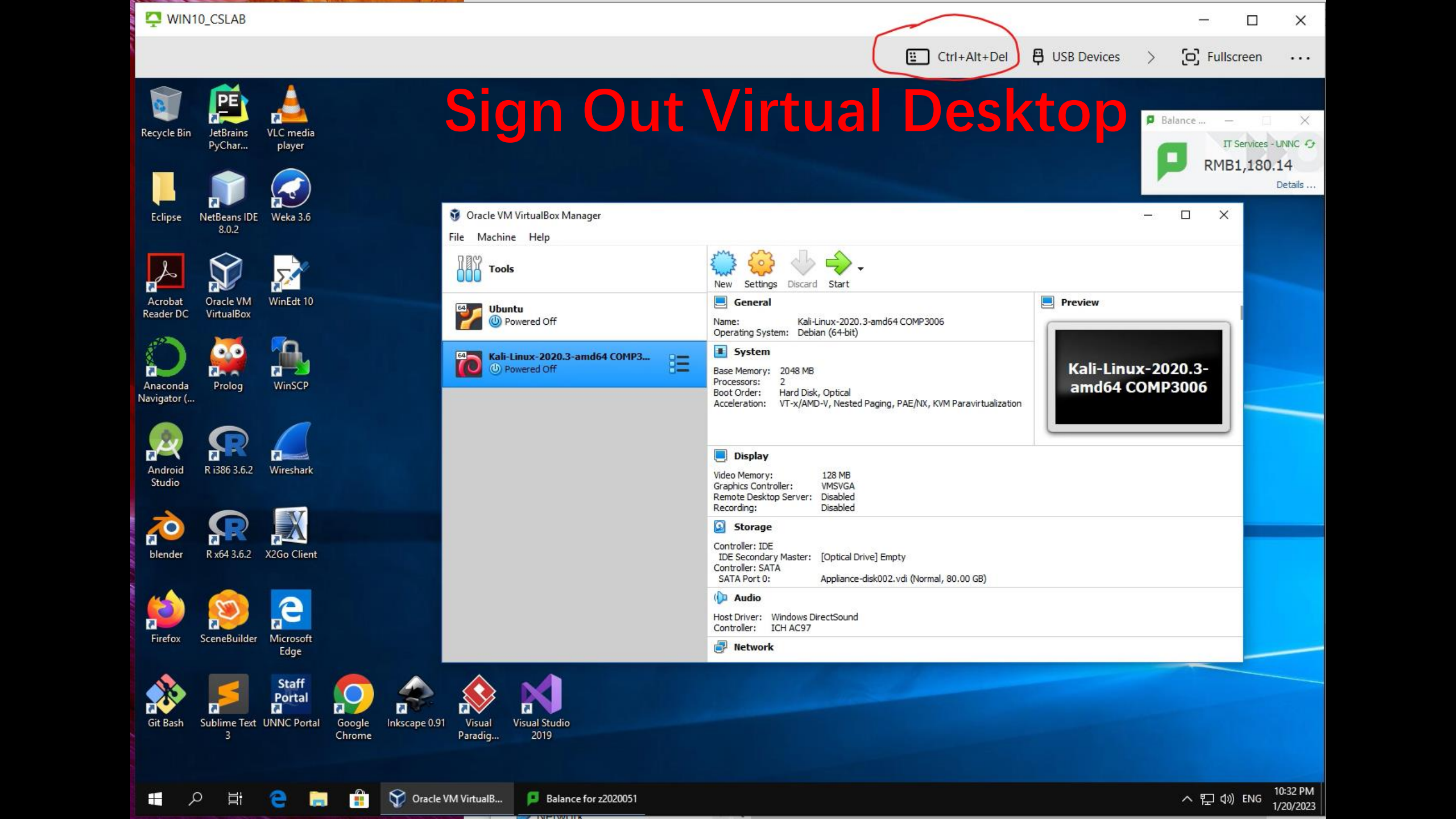

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
09:07 AM
sec@kali: ~/lab1
File Actions Edit View Help
sec@kali:~/lab1$
sec@kali:~/lab1$ nano authscript.sh
sec@kali:~/lab1$ ls -l
total 21164
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
-rwxr-xr-x 1 sec sec 242 Jan 20 09:03 authscript.sh
sec@kali:~/lab1$ ./authscript.sh > baddies
Run Script to Display Unique Combinations of Username and IP & Redirect Output to File baddies
It may take a few minutes to complete.
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
10:07 PM
1/20/2023

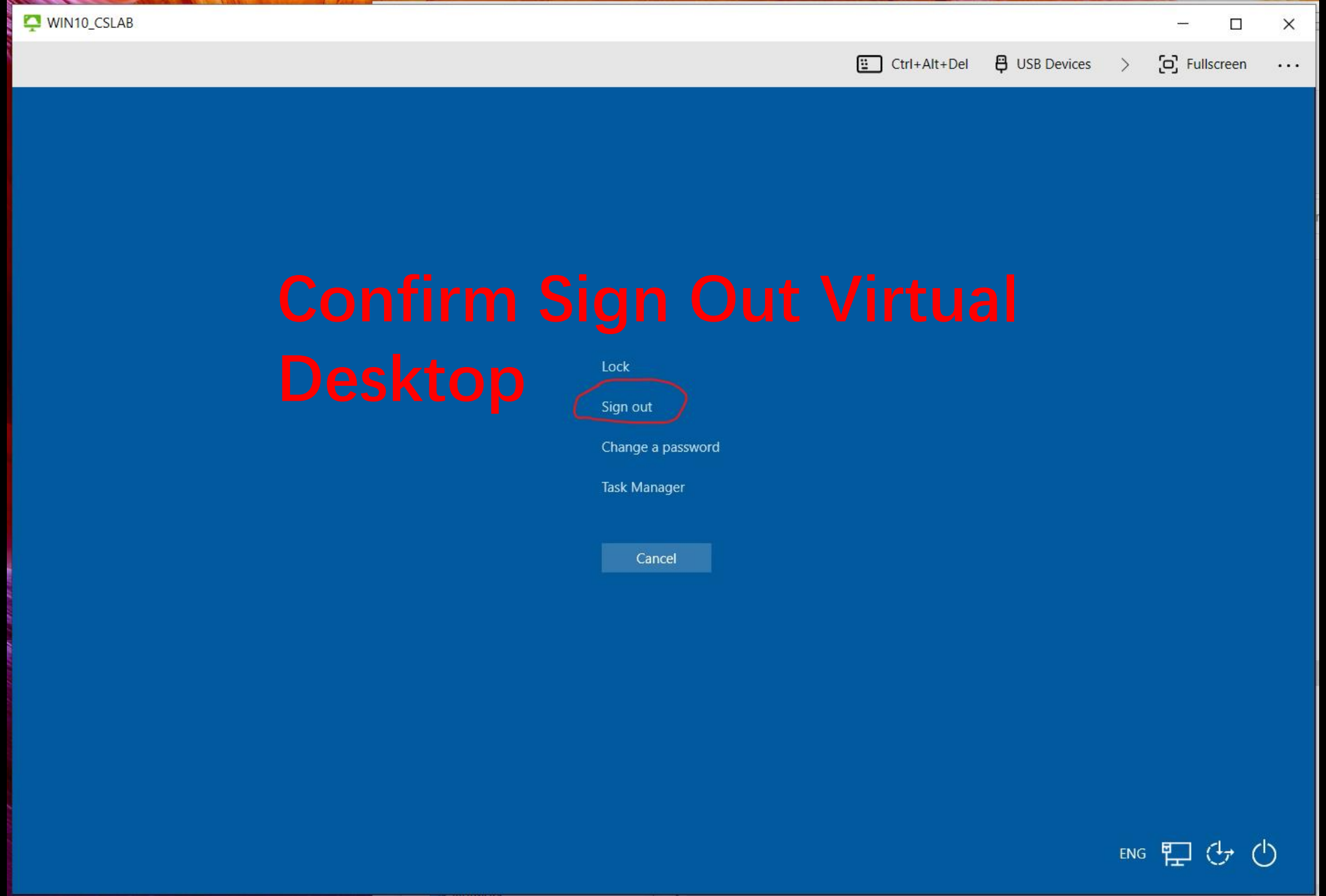

WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
09:20 AM
sec@kali: ~/lab1
File Actions Edit View Help
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ ls -l
total 21300
-rw-r--r-- 1 sec sec 21664135 Nov 17 2020 auth.log
-rwxr-xr-x 1 sec sec 242 Jan 20 09:03 authscript.sh
-rw-r--r-- 1 sec sec 138112 Jan 20 09:05 baddies
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ cat baddies | head -n 100
1:199.89.55.183
12:199.89.55.183
123:115.231.209.245
123:121.244.210.194
123:122.155.201.20
123:190.85.220.40
123:199.89.55.183
1234:122.155.201.20
1234:199.89.55.183
12345:199.89.55.183
123456:115.231.209.245
123456:121.244.210.194
123456:190.85.220.40
123456:199.89.55.183
123456:54.223.240.50
123456:54.223.62.240
1234567:199.89.55.183
12345678:199.89.55.183
123456789:199.89.55.183
123:54.223.240.50
123:54.223.62.240
1:94.79.33.21
1q:122.155.201.20
2:122.155.201.20
2:199.89.55.183
22:192.74.242.129
3:199.89.55.183
3nagios:31.184.195.115
4:199.89.55.183
Display First 100 Lines of File baddies with Combinations of Username and IP
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
10:20 PM
1/20/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab1
11:26 AM
sec@kali: ~/lab1
File Actions Edit View Help
sec@kali:~/lab1$
exit
Exit User Account and
Terminal Emulator Mode
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
12:26 AM
1/22/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
11:40 AM
Trash
File System
Home
Sign Out Kali-Linux System
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
12:40 AM
1/22/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
11:46 AM
Trash
File System
Home
Select Shut Down Virtual Machine
Log out Security
Log Out
Restart
Shut Down
Suspend
Hibernate
Hybrid Sleep
Switch User
Save session for future logins
Cancel
Right Ctrl
Oracle VM VirtualB...
Balance for z2020051
Kali-Linux-2020.3-a...
ENG
12:46 AM
1/22/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Sign Out Virtual Desktop
Recycle Bin
JetBrains PyChar...
VLC media player
Eclipse
NetBeans IDE 8.0.2
Weka 3.6
Acrobat Reader DC
Oracle VM VirtualBox
WinEdt 10
Anaconda Navigator (...
Prolog
WinSCP
Android Studio
R i386 3.6.2
Wireshark
blender
R x64 3.6.2
X2Go Client
Firefox
SceneBuilder
Microsoft Edge
Git Bash
Sublime Text 3
UNNC Portal
Google Chrome
Inkscape 0.91
Visual Paradig...
Visual Studio 2019
Balance ...
IT Services - UNNC
RMB1,180.14
Details ...
Oracle VM VirtualBox Manager
File Machine Help
Tools
Ubuntu
Powered Off
Kali-Linux-2020.3-amd64 COMP3...
Powered Off
New Settings Discard Start
General
Name: Kali-Linux-2020.3-amd64 COMP3006
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Preview
Kali-Linux-2020.3-amd64 COMP3006
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Appliance-disk002.vdi (Normal, 80.00 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
Oracle VM VirtualB...
Balance for z2020051
ENG
10:32 PM
1/20/2023


WIN10_CSLAB
Ctrl+Alt+Del
USB Devices
Fullscreen
Confirm Sign Out Virtual Desktop
Lock
Sign out
Change a password
Task Manager
Cancel
ENG

Exercise

- Try to understand the following Linux script (program).

```
regex="(\S+) from (([0-9]{1,3}\.){3}[0-9]{1,3})"
cat auth.log | grep -E 'sshd.*Failed password' | while read -r line ;
do
    if [[ $line =~ $regex ]] ;
    then
    echo "${BASH_REMATCH[1]}:${BASH_REMATCH[2]}"
    fi
done | sort | uniq
```

- References:

(1) COMP3052.SEC Getting Started with Kali by Mike Pound, Pages 6-8. (Can be downloaded from Moodle)

(2) What does `while read -r line || [[ -n $line ]]` mean?

- https://unix.stackexchange.com/questions/478720/what-does-while-read-r-line-n-line-mean

(3) How to Use Regular Expressions (RegEx) on Linux?

- https://www.geeksforgeeks.org/how-to-use-regular-expressions-regex-on-linux/