TTM4175 Introduction to Communication Technology and data security

Introduction to Kali linux

Laszlo Erdödi

laszlo.erdodi@ntnu.no

Lecture Overview

- Installing Kali linux
- Using Kali (some examples)

Linux distribution with preinstalled hacking tools

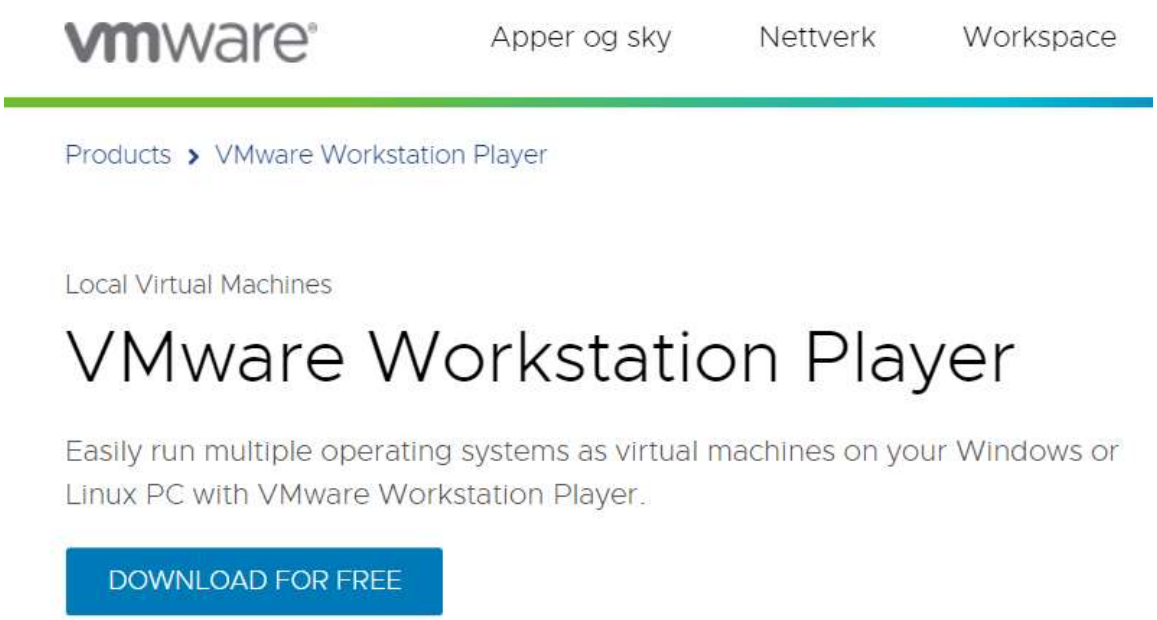
Kali Linux (http://kali.org)

- Debian based Linux distribution with hundreds of preinstalled hacking tools
- Easy to use, tools are classified according to the hacking tasks and steps (info gathering, forensics, vulnerability assessment, etc.)
- Easy to install (ready and up-up-to-date Vmware and Virtualbox images)

Installing Virtualbox

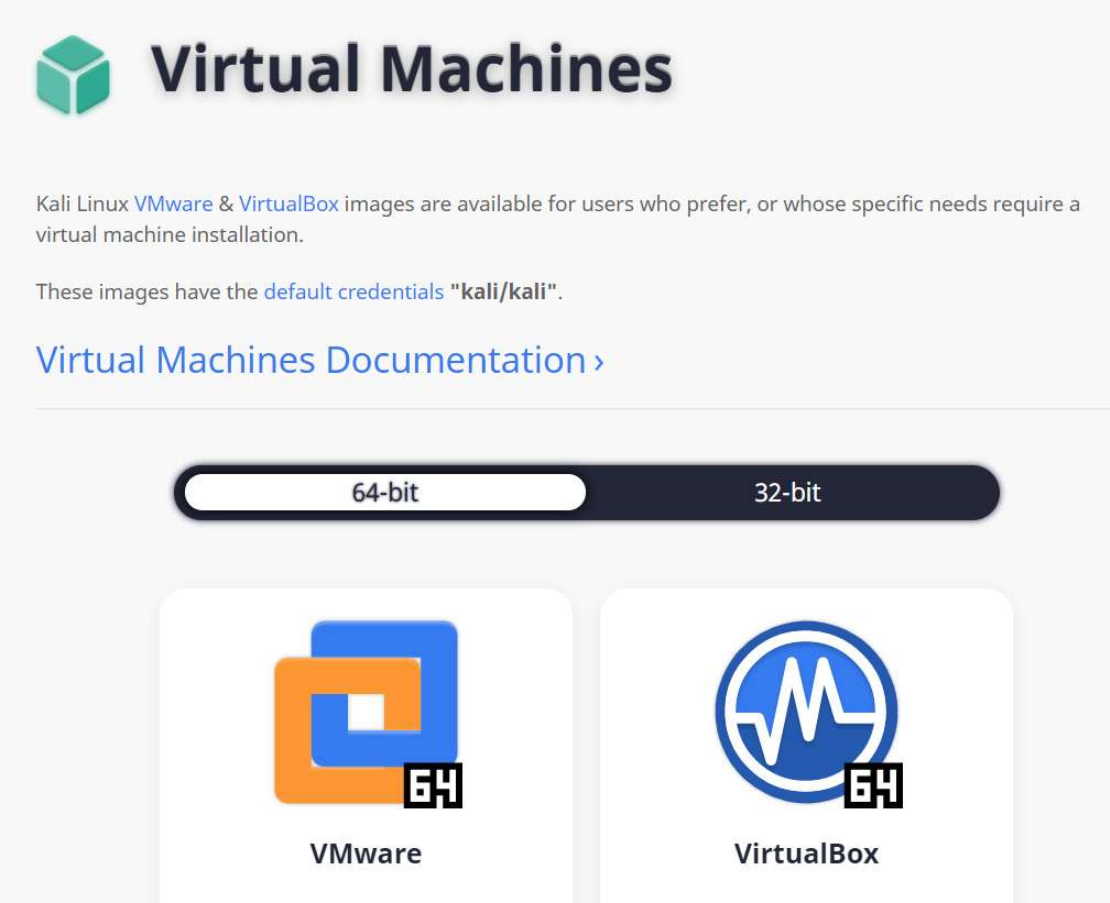
- Download the appropriate platform package: https://www.virtualbox.org/wiki/Downloads
- Launch the installer and follow the steps

Installing Vmware



- Download the appropriate platform package: https://www.vmware.com/no/products/workstation-player.html
- Launch the installer and follow the steps

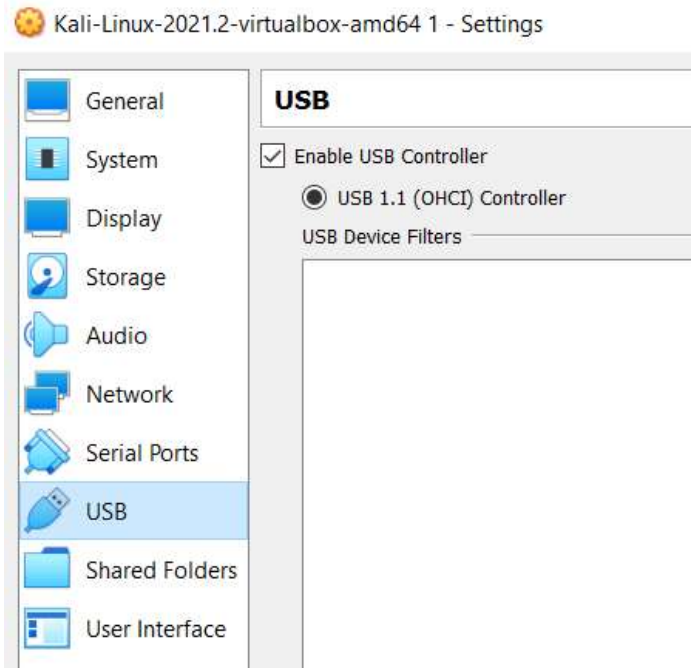
Downloading Kali linux custom image



- Download the 64bit platform for your virtualization platform: https://www.kali.org/get-kali/#kali-virtual-machines
- Click on the ova (Virtualbox) / vmx (Vmware) file to create the virtual machine

Typical problems with Kali linux installation

- USB compatibility
- Virtualization in disabled in BIOS (Intel VT-x, AMD-v)
- HyperV should be disabled sometimes

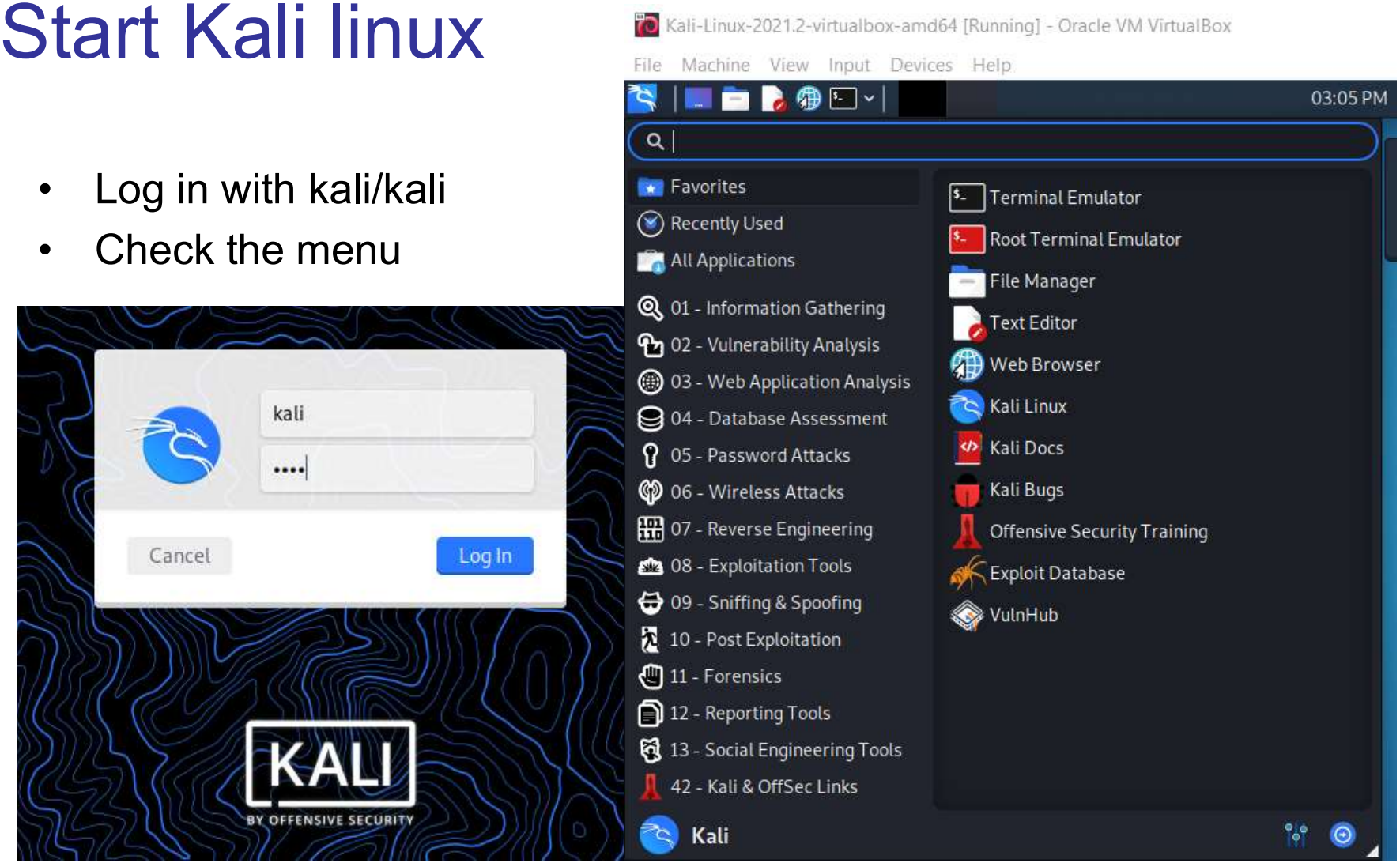


Typical problems with Kali linux installation

- USB compatibility
- Virtualization in disabled in BIOS (Intel VT-x, AMD-v)
- HyperV should be disabled sometimes

Start Kali linux

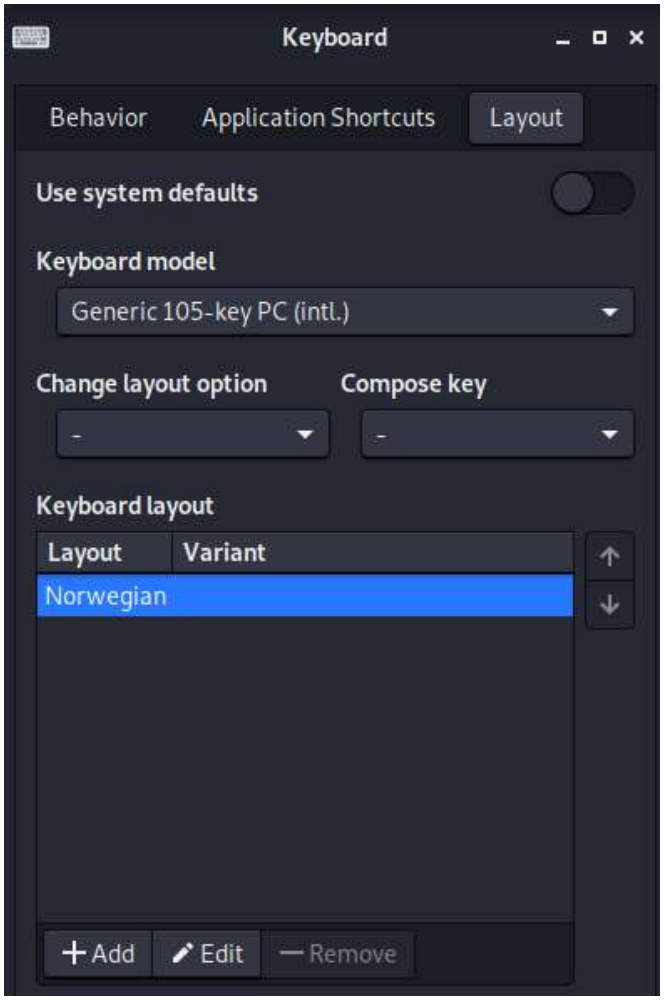
- Log in with kali/kali
- Check the menu



Adding Norwegian keyboard layout

- Type keyboard in the search field
- Open the Keyboard
- Click on Layout and Add
- Find the Norwegian from the list
- Remove English

- Or use the terminal and type:
  setxkbmap no ☺



Use the terminal for file management

- Try the following commands
  - ls, cd, mkdir, touch
  - locate, chmod
- Check the manual of the instructions
- Try the previous commands with parameters

Try curl and grep

```
┌──(kali㉿kali)-[~]
└─$ curl http://hackingarena.com/home/index.html | grep \<a
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  7074  100  7074                    <a href="https://www.uio.no/english/" class="uio-seal" tabindex="-1">
                <a href="https://www.hackingarena.no" class="uio-acronym georgia">UiO</a>
                <a href="https://www.hackingarena.no" class="uio-host uio-host-resp" tabindex="-1">University of Oslo</a>
                <a href="https://www.hackingarena.no" class="uio-host">Hacking Arena</a>
                <!-- <a href="https://www.hackingarena.no" class="uio-faculty georgia" style="position: relative; left: 18
 0     0                  <a href="./">Home</a>
                <a href="../challenges">Challenges</a>
                <a href="../trainings">Trainings</a>
  177k      0 --:--:-- --:--:-- --:--:--  177k
                <a href="../research">Research</a>
                <a href="../contact">Contact us</a>
                <a href="../signin">Sign in</a>
          <li class="vrtx-ancestor"> <a href="../trainings"><span>Trainings</span></a></li>
          <li class="vrtx-ancestor"> <a href="../research"><span>Research</span></a></li>
          <li class="vrtx-ancestor"> <a href="../challenges"><span>Challenges</span></a></li>
              <li class="vrtx-child"><a href="../challenges/network"><span>Network reconnaissance</span></a></li>
              <li class="vrtx-child"><a href="../challenges/web"><span>Web hacking</span></a></li>
              <li class="vrtx-child"><a href="../challenges/binary"><span>Binary exploitation</span></a></li>
              <li class="vrtx-child"><a href="../challenges/reverse"><span>Reverse engineering</span></a></li>
              <li class="vrtx-child"><a href="../challenges/forensics"><span>Forensics</span></a></li>
              <li class="vrtx-child"><a href="../challenges/stego"><span>Steganography</span></a></li>
```

Try sudo / check the current user(s)

```
┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root💀kali)-[/home/kali]
└─# whoami
root

┌──(root💀kali)-[/home/kali]
└─# exit

┌──(kali㉿kali)-[~]
└─$ whoami
kali

┌──(kali㉿kali)-[~]
└─$
```

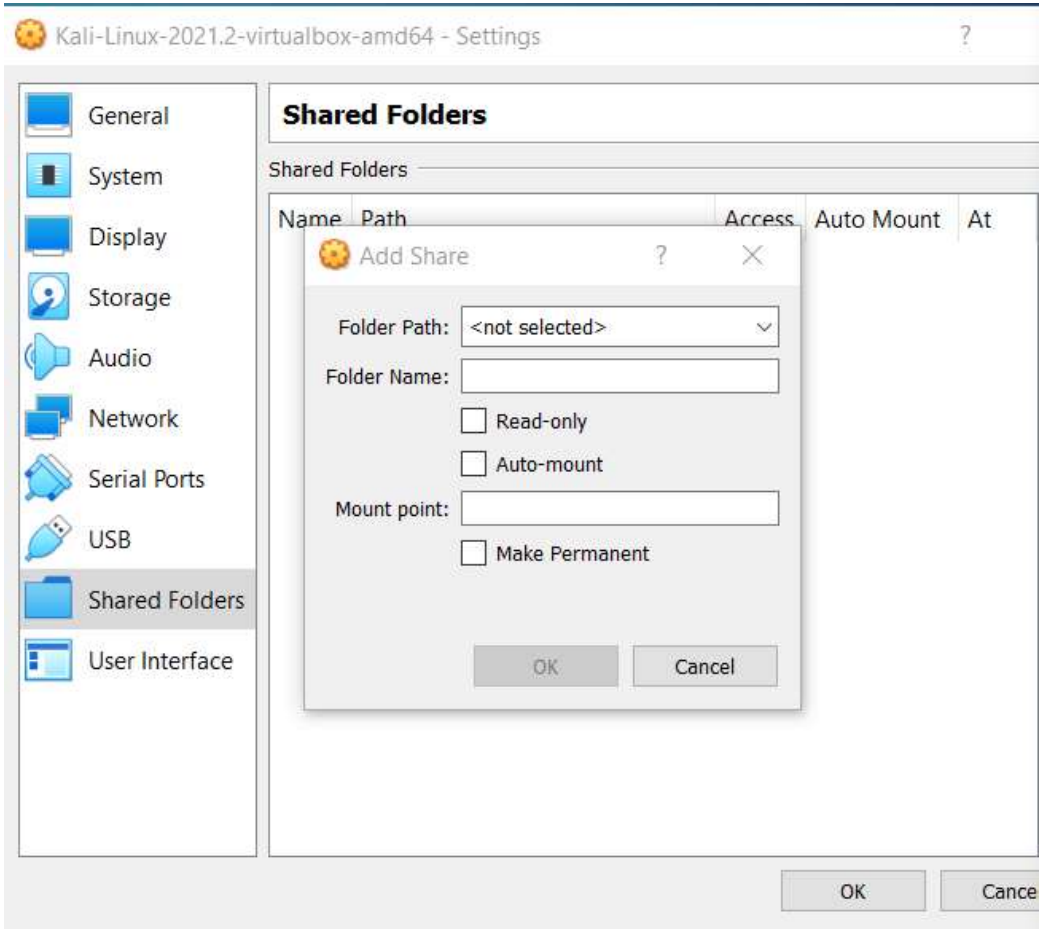
```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:112::/nonexistent:/usr/sbin/nologin
messagebus:x:108:113::/nonexistent:/usr/sbin/nologin
redsocks:x:109:114::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:111:65534::/run/iodine:/usr/sbin/nologin
miredo:x:112:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin
usbmux:x:114:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tcpdump:x:115:121::/nonexistent:/usr/sbin/nologin
```

Find and install packages

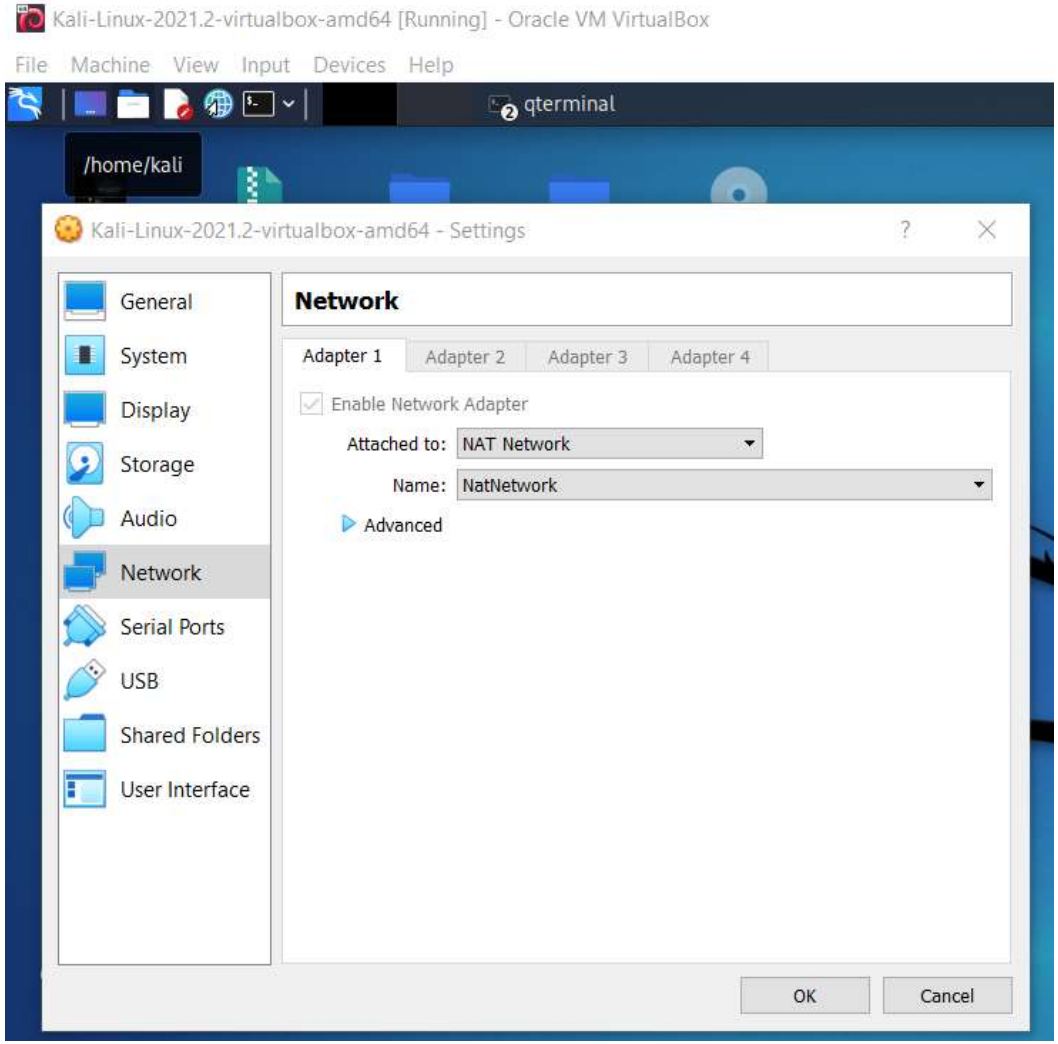
```
┌──(kali㉿kali)-[~]
└─$ apt-cache search python | grep exploit
powershell-empire - PowerShell and Python post-exploitation agent
python3-pyexploitdb - library to fetch the most recent exploit-database (Python 3)
silenttrinity - asynchronous, collaborative post-exploitation agent
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install gdb-peda
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  gdb-peda
0 upgraded, 1 newly installed, 0 to remove and 16 not upgraded.
Need to get 61.3 kB of archives.
After this operation, 322 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/non-free amd64 gdb-peda amd64 1.1~20180207-0kali2 [61.3 kB]
Fetched 61.3 kB in 1s (74.6 kB/s)
Selecting previously unselected package gdb-peda.
(Reading database ... 287817 files and directories currently installed.)
Preparing to unpack .../gdb-peda_1.1~20180207-0kali2_amd64.deb ...
Unpacking gdb-peda (1.1~20180207-0kali2) ...
Setting up gdb-peda (1.1~20180207-0kali2) ...
```

Create a shared folder



Create a NAT network with 2 Kali VMs



End of lecture