NYU TANDON SCHOOL OF ENGINEERING

NYU Cyber Fellows
CS GY 6573
Penetration Testing

Lab 1 - Getting Started with VirtualBox and Kali

Goal

- **The goal of this lab is to get Kali Linux up and running**

- **We can do this using virtualization, using a live USB or DVD, or setting up Kali in the cloud (Amazon EC2)**

- **For this class, it would be best to virtualize**
  - We will be deploying other VMs (*.ova files) later this semester *at the same time as Kali*
  - By virtualizing, we'll have the easiest experience of managing several hosts that need to be online and networked

- **Once Kali is set up, we will also deploy Metasploitable**
  - Metasploitable will be a common target we'll use through the semester

NYU TANDON SCHOOL OF ENGINEERING

Setup Virtual Environment

Virtualizing

- **We will be running VMs in this class for labs, assignments, and the final project**

- **I recommend VirtualBox - it's free and runs well on most platforms**
  - You can use VMware or any other hypervisor your want, but you may have issues getting the OVAs to deploy and networked correctly

- **Your system should meet the minimum requirements:**
  - https://www.virtualbox.org/wiki/End-user_documentation
  - Any reasonably powerful x86 hardware
  - 8GB of RAM (16GB recommended)
  - About 30GB free space

VirtualBox

- https://www.virtualbox.org/wiki/Downloads

VirtualBox

Login Preferences

Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

About
Screenshots
Downloads
Documentation
End-user docs
Technical docs
Contribute
Community

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 6.0 packages, see VirtualBox 6.0 builds. Please also use version 6.0 if you need to run VMs with software virtualization, as this has been discontinued in 6.1. Version 6.0 will remain supported until July 2020.

If you're looking for the latest VirtualBox 5.2 packages, see VirtualBox 5.2 builds. Please also use version 5.2 if you still need support for 32-bit hosts, as this has been discontinued in 6.0. Version 5.2 will remain supported until July 2020.

VirtualBox 6.1.2 platform packages

- Windows hosts
- OS X hosts
- Linux distributions
- Solaris hosts

The binaries are released under the terms of the GPL version 2.

See the changelog for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages. *The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!*

- SHA256 checksums, MD5 checksums

Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

VirtualBox 6.1.2 Oracle VM VirtualBox Extension Pack

- All supported platforms

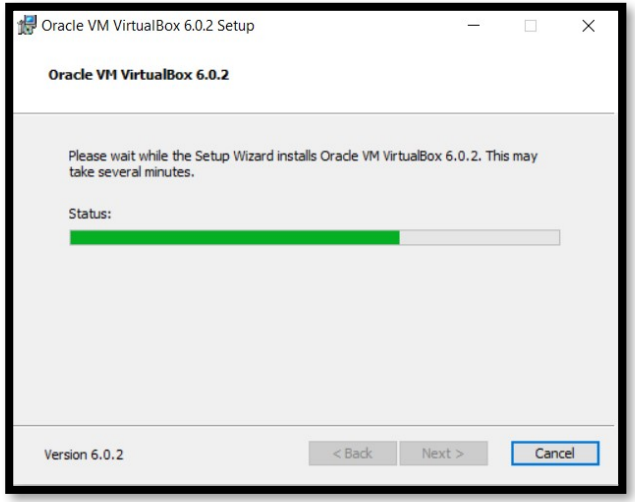
Support for USB 2.0 and USB 3.0 devices, VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See this chapter from the User Manual for an introduction to this Extension Pack. The Extension Pack binaries are released under the VirtualBox Personal Use and Evaluation License (PUEL). *Please install the same version extension pack as your installed version of VirtualBox.*

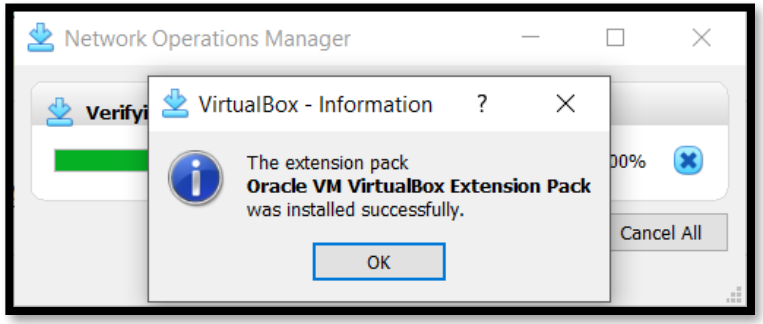
1- Download & Install

2 - Install Extension Pack

Virtualbox Install

- **Windows and Mac**
  - Use default options, installation is straight forward and should have no issues
- **Linux**
  - Follow instructions based on your distribution
  - https://www.virtualbox.org/wiki/Linux_Downloads





Don't forget to install the Extension Pack!

Vmware Player

- https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html

- **Only Windows and Linux**

- **No free version for OSX**
  - VMWare Fusion is the alternative if you have a license

NYU TANDON SCHOOL OF ENGINEERING

Networking

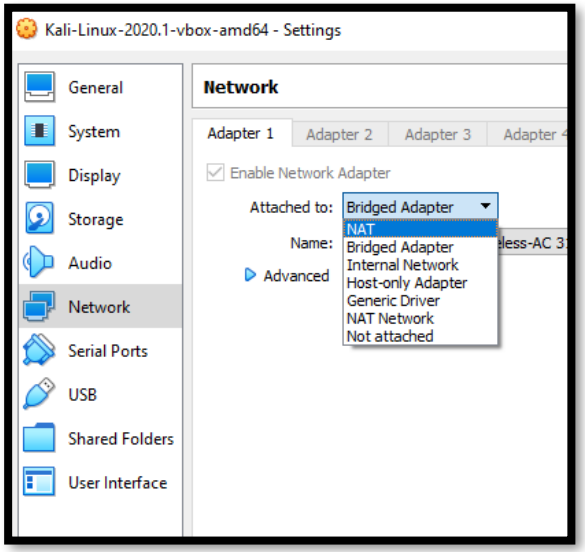
Networking Types

- **There are several types of network options for deployed VMs**
  - With all options, VMs on the same network should be able to communicate to each other

- **NAT**
  - Host machine becomes an internet gateway
  - VM has internet access
  - Host machine cannot communicate to VM without port forwarding
  - Good for “normal” use

- **Bridged**
  - Host machine forwards all traffic to LAN gateway
  - VM and Host are on the same LAN
    - Different IP addresses but share a MAC address
  - VMs can communicate to one another
  - Preferred if doing any kind of scanning or exploiting externally

- **Internal/Host-only**
  - VMs cannot access the internet
  - Internal means the host cannot communicate to the VM
  - Both Internal and Host-only, VMs can communicate to each other
  - Best if running vulnerable target VMs, no internet access required

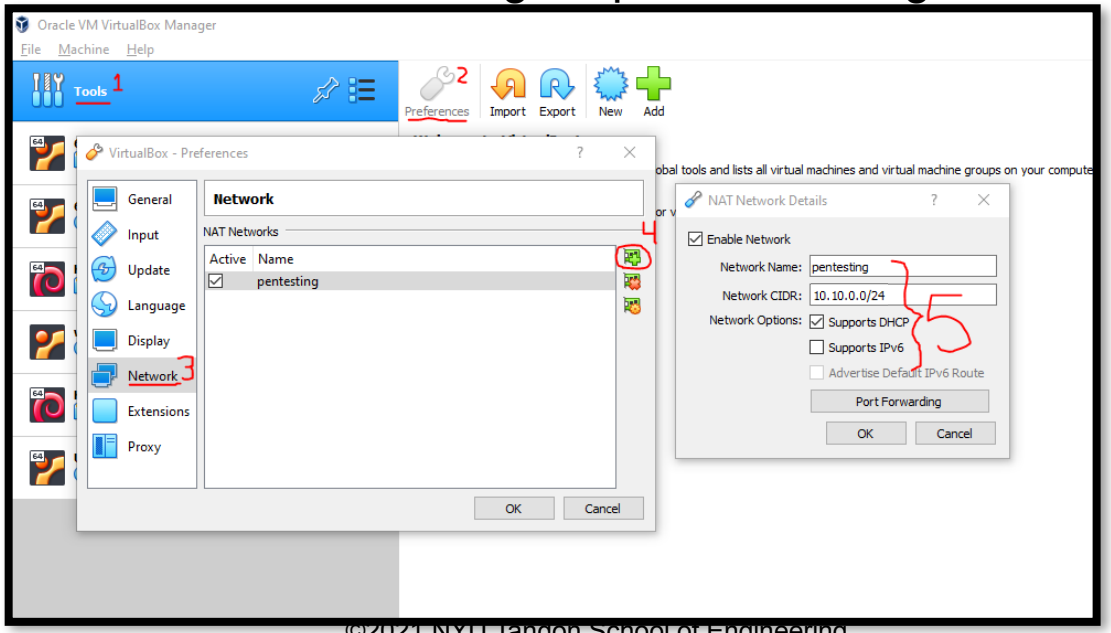


Lab Network

- **How you set up networking is up to you but remember that we will be using hacking tools and deploying dangerous/vulnerable VMs**
- **The slides will explain how to use NAT**
- **It doesn't matter which option you choose, as long as the VMs can communicate on the same subnet AND it is secure**
- **If you are in your own private network behind a NAT gateway (like a router), it may be safe to just set it up on your own LAN in bridged mode**
  - Remember that anything you deploy will be vulnerable to anything that is hostile on your network

Create a NAT network Windows

- **Create a new NAT network**
  - Call it anything
  - Set its network to 10.10.0.0/24
  - No need to enable IPv6 or configure port forwarding for now



Create a NAT Network Mac OSX

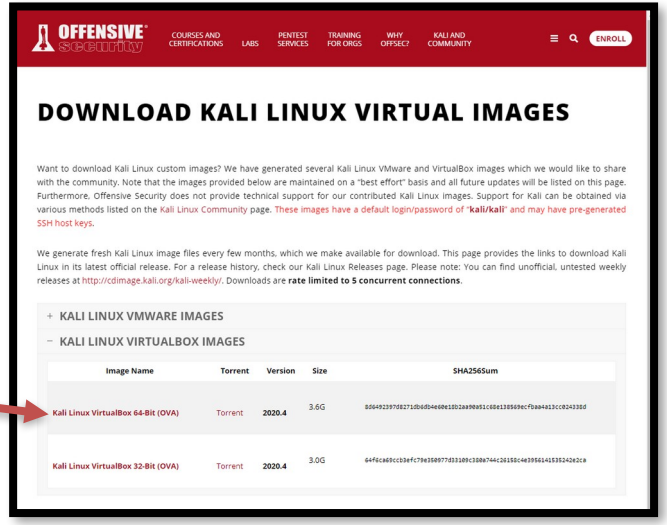
- You will not have a Tools option
- Instead go to
  - VirtualBox > Preferences > Network
- Follow the same instructions

NYU TANDON SCHOOL OF ENGINEERING

Deploy Kali, virtual

- **You can download premade versions of Kali for VirtualBox or VMWare**
  - Use the 64-bit version
  - https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

Latest 64-bit version



OFFENSIVE security | COURSES AND CERTIFICATIONS | LABS | PENTEST SERVICES | TRAINING FOR ORGS | WHY OFFSEC? | KALI AND COMMUNITY | ENROLL

DOWNLOAD KALI LINUX VIRTUAL IMAGES

Want to download Kali Linux custom images? We have generated several Kali Linux VMware and VirtualBox images which we would like to share with the community. Note that the images provided below are maintained on a "best effort" basis and all future updates will be listed on this page. Furthermore, Offensive Security does not provide technical support for our contributed Kali Linux images. Support for Kali can be obtained via various methods listed on the Kali Linux Community page. These images have a default login/password of "**kali/kali**" and may have pre-generated SSH host keys.

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at http://cdimage.kali.org/kali-weekly/. Downloads are **rate limited to 5 concurrent connections**.

+ KALI LINUX VMWARE IMAGES

− KALI LINUX VIRTUALBOX IMAGES

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux VirtualBox 64-Bit (OVA)	Torrent	2020.4	3.6G	8d649239708271db6d54e60e18D2aa90a91c60e138569ecfbab4a13cc024338d
Kali Linux VirtualBox 32-Bit (OVA)	Torrent	2020.4	3.0G	64f6ca69ccb3efc79e350977d33109c380a744c2015Dc4e39561415352420c2ca

Import the Kali Image

- Open VirtualBox
- File -> Import Appliance -> Select the *.ova file

- It should be intuitive

- If you need help, ask questions on Slack

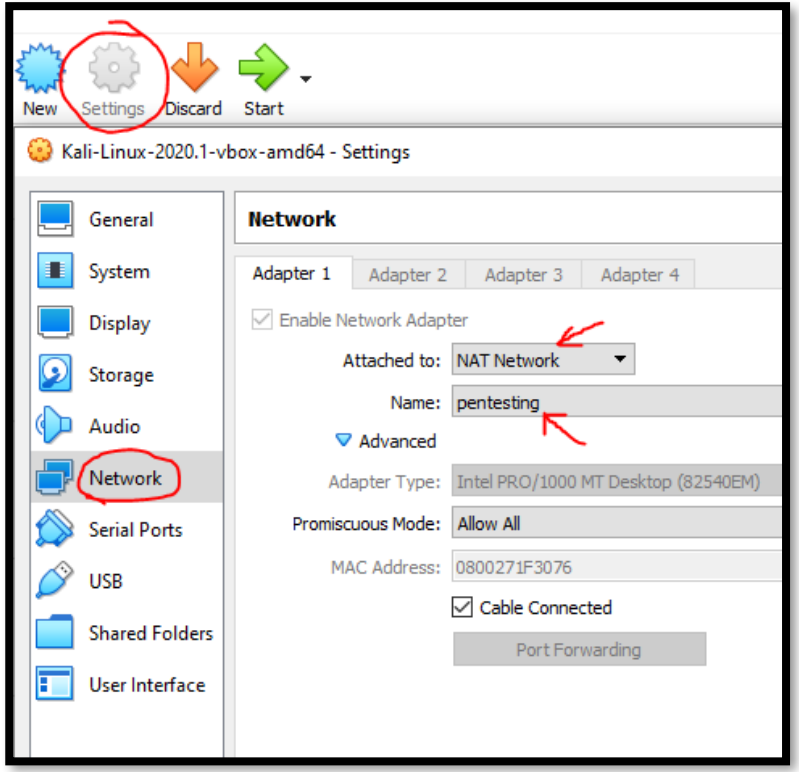
- A good tutorial:
  - https://www.maketecheasier.com/import-export-ova-files-in-virtualbox/

Change Network Settings

- **We need to go to**
  - Machine -> Settings
  - Network tab
  - Attach to NAT network
    - Select the NAT you created

- **We want to reach the internet and also communicate with other VMs**

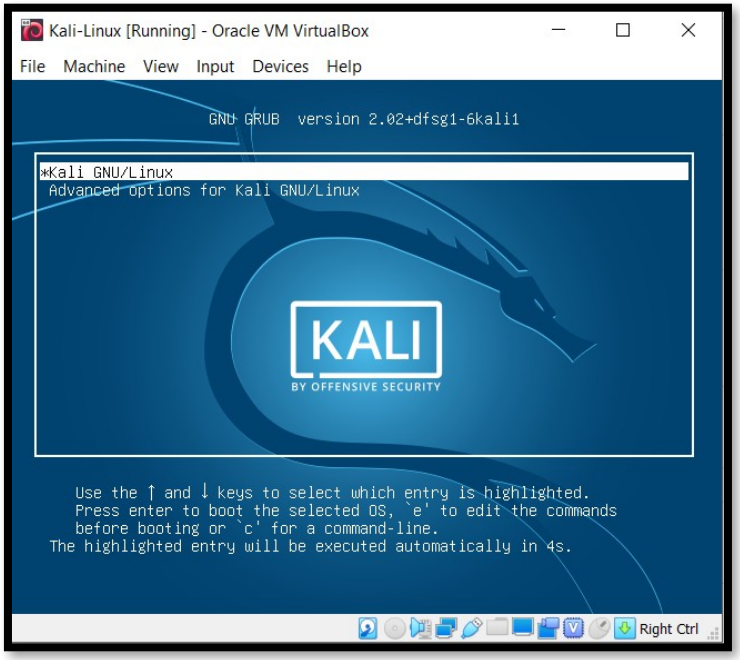
- **This is safer than Bridged**
  - Do not deploy dangerous or vulnerable VMs to a LAN unless you trust it and own it



Start Kali

- **Default option, press enter**

- **User**
  - kali
- **Password**
  - kali



- **Troubleshooting:**
  - Make sure you install the extension pack

Kali Tools and Metapackage

- **Kali organizes many of its tools and packages into Metapackages**

- **Metapackages are a way to link or group many similar tools**

- **This keeps instances of Kali lightweight if only a specific toolset is needed**
  - Examples are **kali-linux-wireless** or **kali-linux-headless**

- **Kali VM includes some tools and packages, found in these metapackages**
  - kali-linux-core
  - Kali-linux-default

- **If installing manually or want to add additional metapackages, please review the tool and metapackage list page for the latest details:**
  - https://tools.kali.org/kali-metapackages

- **More info:**
  - https://www.kali.org/news/major-metapackage-makeover

NYU TANDON SCHOOL OF ENGINEERING

Metasploitable

Metasploitable

- **Metasploitable 2 is an Ubuntu distribution released by Rapid7**
- **Its purpose is to be vulnerable and let us practice!**
- **Direct Download:**
  - http://downloads.metasploit.com/data/metasploitable/metasploitable-linux-2.0.0.zip
  - Or sourceforge mirrors:
  - https://sourceforge.net/projects/metasploitable/

- **Metasploitable has been around since 2012 and is well documented**
- **Troubleshooting should be easy. If any issues completing anything in this lab, research first, then ask questions**

Network Setup - VirtualBox

- **Future labs will require that we use VirtualBox since there is no version of Metasploitable ready and available AWS**
  - AWS only allows penetration testing of medium systems (you need to pay $$$) and also get explicit authorization

- **It should NEVER be allowed to face the open internet**
  - This system's purpose is to get scanned and hacked
  - Exposing to the internet will probably turn it into a bitcoin mining host within a day

- **Security - We should use NAT, Host-only, or Internal networking**
  - This will allow our VMs and host to communicate internally
  - Alternatively, we can whitelist IP addresses using iptables

NYU TANDON SCHOOL OF ENGINEERING

Deploying Metaploitable

Setup

- **You are to deploy the image to your local machine**
  - You will need to configure VirtualBox, VMware, etc.
    - Your host-only interface needs to be setup so you are on the same network
  - <u>Do not expose this VM to the internet or an untrusted network - it's vulnerable</u>

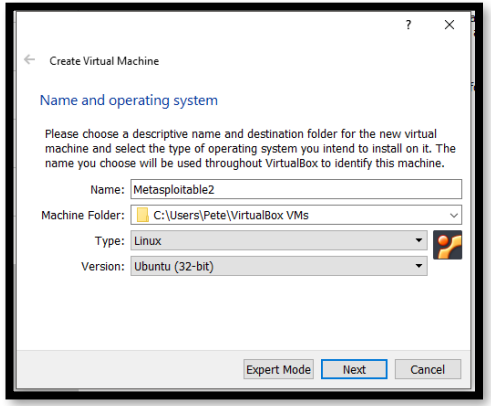
- **The next few slides we will:**
  1. Deploy VM
  2. Set up host-only networking
  3. Configure Kali and the VM

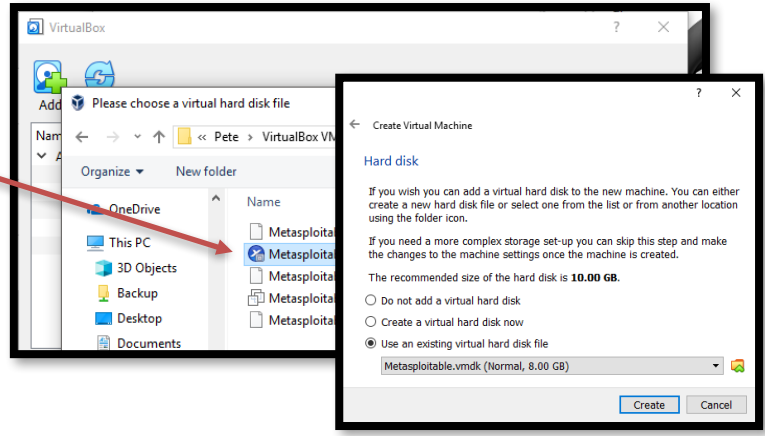
Metasploitable

- **Download and Unzip metasploitable-linux-2.0.0.zip**

- **Instructions for deploying in Virtualbox:**
  - Open VirtualBox
  - Machine->New... (Ctrl+N)
    - Name:Metasploitable
    - Type: Linux
    - Version: Ubuntu 32-bit
    - Default RAM
    - Use existing virtual hard disk -> Metasploitable.vmdk
      - You will need to manually add it
  - Start VM
  - Username and password are both '**msfconsole**'

- **Stuck with keyboard-only input on a small screen**
- **You can SSH into it on a GUI for a more friendly interface if required**



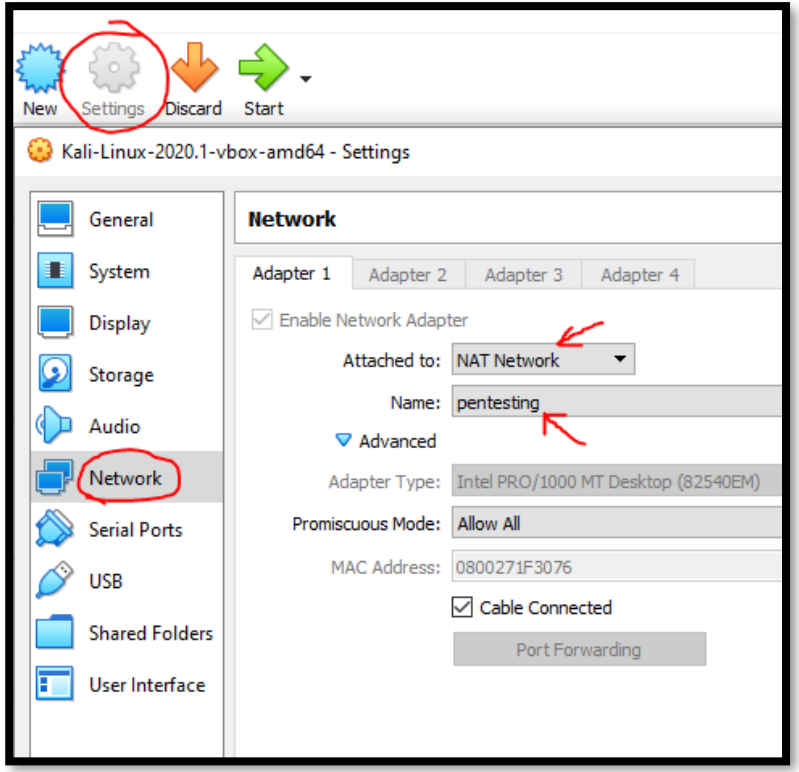


Change Network Settings

- **Just like Kali - we need to go to**
  - Machine -> Settings
  - Network tab
  - Attach to NAT network
    - Select the NAT you created

- **We want to reach the internet and also communicate with other VMs**

- **This is safer than Bridged**
  - Do not deploy dangerous or vulnerable VMs to a LAN unless you trust it and own it



Networking

- Start the Metasploitable and Kali VMs
- Once they are both on, make sure the IPs on the same subnet so they can communicate
- You can use a different network address for your host-only network
- All the examples in this lab will assume you are using 10.10.0.0/24
- Next: Setup your IP addresses

Metasploitable Setup

- **Login, escalate privs, and set IP**
  - Login with '**`msfadmin`**' as user and pass
  - Become root
    - **`$ sudo su -`**
      - Enter password again: **msfadmin**
  - Check name of network adapter
    - Probably 'eth0' but could vary
  - **`# ifconfig`**
- Set your IP where [name] is your adapter, probably eth0!
    - **`# dhclient [name]`**

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin_
```

```
msfadmin@metasploitable:~$ sudo su -
[sudo] password for msfadmin:
root@metasploitable:~# ifconfig _
```

```
root@metasploitable:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:44:ae:b3
          inet addr:10.10.0.20  Bcast:10.10.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe44:aeb3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2424 (2.3 KB)  TX bytes:5066 (4.9 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)
```

Kali Setup

- **On Kali**
  - Try to ping Metasploitable from Kali to make they are connected.
  - Troubleshooting?
    - Try turning the network adapter off and back on again.

Ping to check

- **Ping both ways...success!**

```
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:d4:4c:82 brd ff:ff:ff:ff:ff:ff
    inet 10.10.0.10/24 brd 10.10.0.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fed4:4c82/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
kali@kali:~$ ping 10.10.0.20
PING 10.10.0.20 (10.10.0.20) 56(84) bytes of data.
64 bytes from 10.10.0.20: icmp_seq=1 ttl=64 time=0.230 ms
64 bytes from 10.10.0.20: icmp_seq=2 ttl=64 time=0.209 ms
^C
--- 10.10.0.20 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.209/0.219/0.230/0.010 ms
```

```
root@metasploitable:~# ping 10.10.0.10
PING 10.10.0.10 (10.10.0.10) 56(84) bytes of data.
64 bytes from 10.10.0.10: icmp_seq=1 ttl=64 time=0.285 ms
64 bytes from 10.10.0.10: icmp_seq=2 ttl=64 time=0.217 ms
64 bytes from 10.10.0.10: icmp_seq=3 ttl=64 time=0.275 ms

--- 10.10.0.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.217/0.259/0.285/0.029 ms
root@metasploitable:~# _
```

NYU TANDON SCHOOL OF ENGINEERING

Networking Issues?

If you try using Bridged

- **Bridged network doesn't work correctly on some public wifi networks!**
  - **Including NYU's wifi**
  - Bridged wifi shares the same physical address of the wlan card for multiple hosts
    - Bridging does not create a new wireless adapter. It shows up in the VM as an ethernet connection
  - Some Access Points can detect multiple hosts using the same MAC address and will only service the first host and MAC

- **This prevents access control attacks**
  - Alice is authenticated to NYU's network using her account credentials
  - Bob wants network access but does not have credentials
  - By configuring his MAC address to copy Alice's, Bob might now have access
    - "Hello, it's still me again, 'Alice'. Can I please have another IP address?"
    - This attack used to work and still often does in some public places like airports and hotels, places that charge for wifi

Lab 1 Issues

- Bridging is needed if we are doing any VM-to-Internet scanning or exploiting in this class
- In your academic research or careers with pen testing, we should always get authorization from our ISP if we are going to do some very bandwidth-intensive pen testing
- NYU's network may not be satisfactory for some activities
- This class will limit our targets to work around bridging limitations
- NAT is satisfactory for accessing class website or other basic tasks

No Ping?

- **Make sure both VMs are attached to the same virtual network interface**
  - E.g. NAT network
- **Make sure both VMs have IPv4 configured to the same network**
  - E.g. 10.10.0.10/24
- **Try resetting network interfaces**
- **Disable DHCP if it works then stops**
- **Post questions and screenshots on Slack!**

Lab 1 Issues - Shared WLAN MAC address issue

- We can see Kali is in bridged mode and has an ethernet interface ending in :df
- This shows up in my wireless router's DHCP table
- The wireless clients shows a different MAC address though, same as host machine "JAKKU"

System Log - DHCP leases

This page shows the device's related settings such as MAC, IP, and lease time settings.

Hostname	IP Address	MAC Address	Expires
kali	192.168.1.229	08:00:27:81:b1:df	23:53:17
JAKKU	192.168.1.204	70:1c:e7:52:ef:81	14:11:31

Client status

Online | Wired (3) | Wireless (3)

jakku

JAKKU
192.168.1.229
70:1C:E7:52:EF:81

kali
192.168.1.204
70:1C:E7:52:EF:81

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,
        inet 192.168.1.229  netmask 25
        inet6 fe80::a00:27ff:fe81
        ether 08:00:27:81:b1:df
        RX packets 84731  bytes 710553
```

≠

NYU TANDON SCHOOL OF ENGINEERING

Optional - Deploy Kali, USB

Kali Download

- **You will not be able to complete the labs or assignments using only a live USB without additional configuration changes – you're on your own!**

- **OPTIONAL**
  - Difficult to virtualize additional machines which will be provided
  - Possible to virtualize provided VMs on a separate host on a secure LAN

- **Download the latest Kali image**
  - https://www.kali.org/downloads/

- **Using a USB, 4GB or higher**
  - Windows
    - Download W32 Disk Imager
    - https://launchpad.net/win32-image-writer
  - Linux, OS X
    - Use the dd command

- **https://docs.kali.org/downloading/kali-linux-live-usb-install**

NYU TANDON SCHOOL OF ENGINEERING

Optional - Amazon EC2

Kali on the Cloud

- **You will not be able to complete the labs or assignments using only AWS without additional configuration changes – you're on your own!**

- **OPTIONAL - You can also create an instance of Kali on AWS**
  - If you are limited by hardware or prefer not to perform pen testing locally
  - Also a good option if you only have a Mac, at least to get started
  - https://www.kali.org/news/kali-linux-aws-cloud/

- **You will need to create an AWS account and provide a credit card for any charges you incur**
  - Unless you qualify for free tier

- **If this is your first account, you may qualify for the "free tier"**
  - 12-months
  - 5GB of storage
  - 750 hours of use per month
    - Must use **t2.micro!**
    - https://aws.amazon.com/s/dm/optimization/server-side-test/free-tier/free_np/

Must select for free tier

directly from the

Version

2016.2, rele

Region

US West (N

EC2 ype

t2.micro
t2.small
t2.medium
m3.medium
m3.large
m3.xlarge
g2.2xlarge
c3.8xlarge
i2.xlarge
i2.2xlarge

Memory	1 GiB
CPU	1 virtual core
Storage	EBS storage only
Platform	64-bit
Network Performance	Low to Moderate
API Name	t2.micro

VPC Settings

Will launch into: subnet-9c97f1f8 (172.31.16.0/20)

EBS General Purpose (SSD) volumes

Free Tier Eligible

EC2 charges for Micro instances are free for up to **750 hours** a month if you qualify for the AWS Free Tier. See details.

Accept Software Terms & Launch with 1-Click

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) and your use of AWS services is subject to the AWS Customer Agreement.

Cost Estimator

$10.80 / month

t2.micro EC2 Instance usage fees

Assumes 24 hour use over 30 days

Software Charges

$0.00 / month

$0.00 hourly software fees for t2.micro

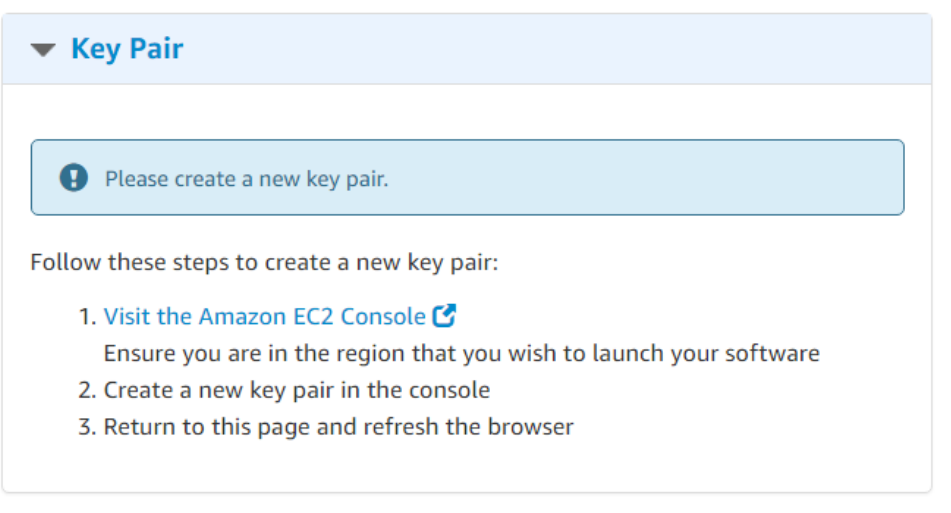
AWS Infrastructure Charges

$10.80 / month

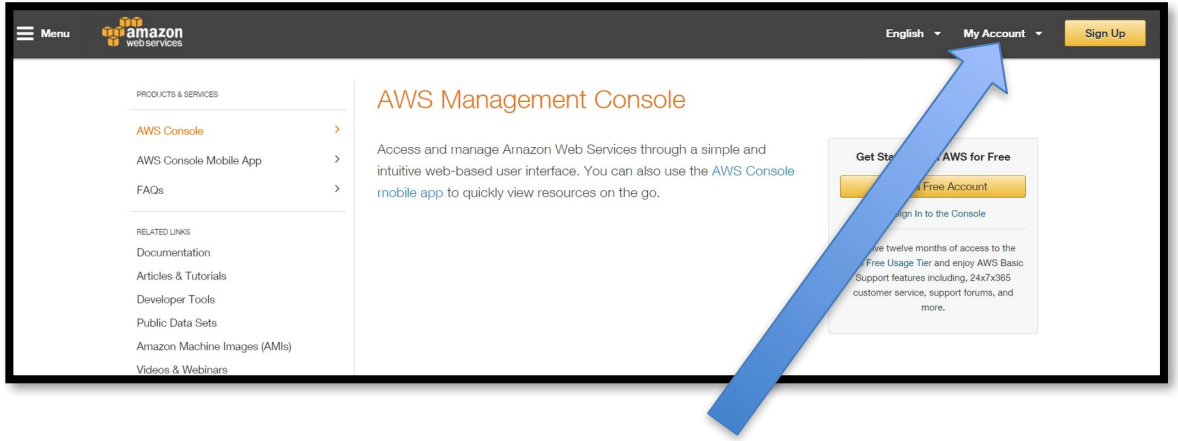
Cost varies for storage fees

$10.80 hourly EC2 instance fees for t2.micro

- Create a new keypair
- You will use this to login over SSH

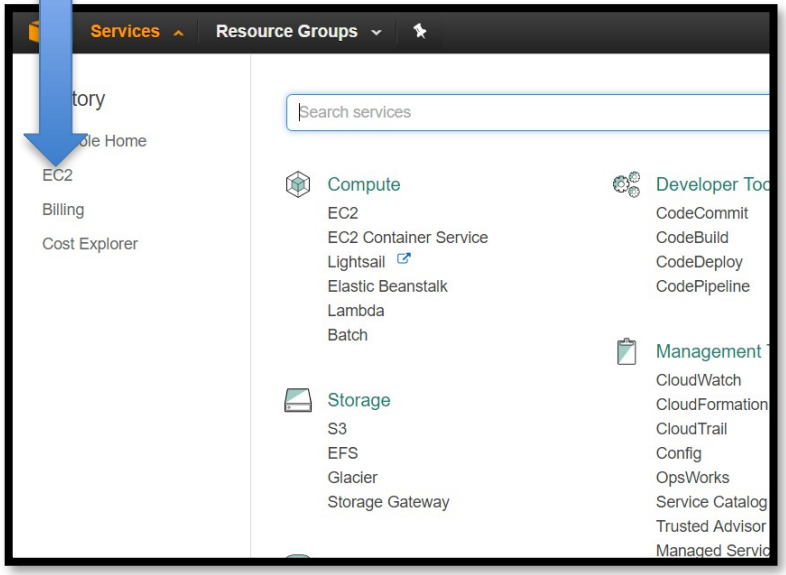


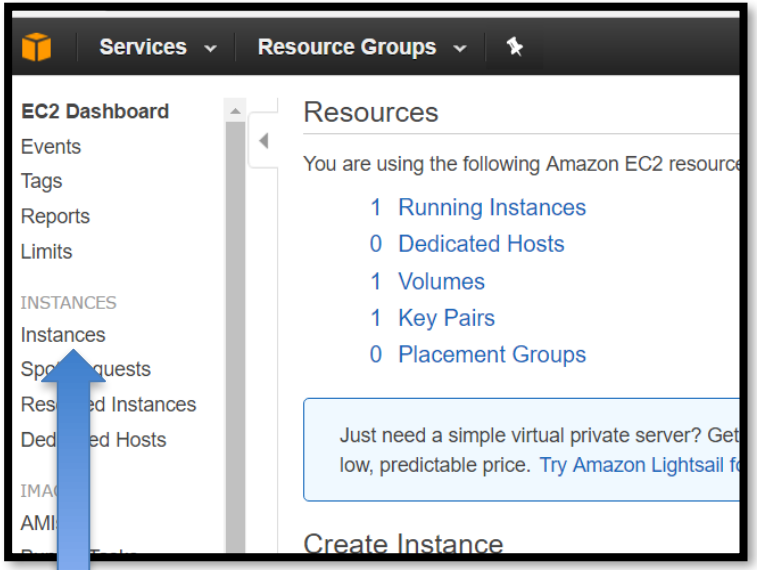
- Go to https://aws.amazon.com/console/



Expand, then click AWS Management Console

Expand services, EC2

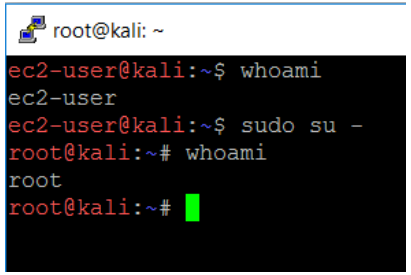


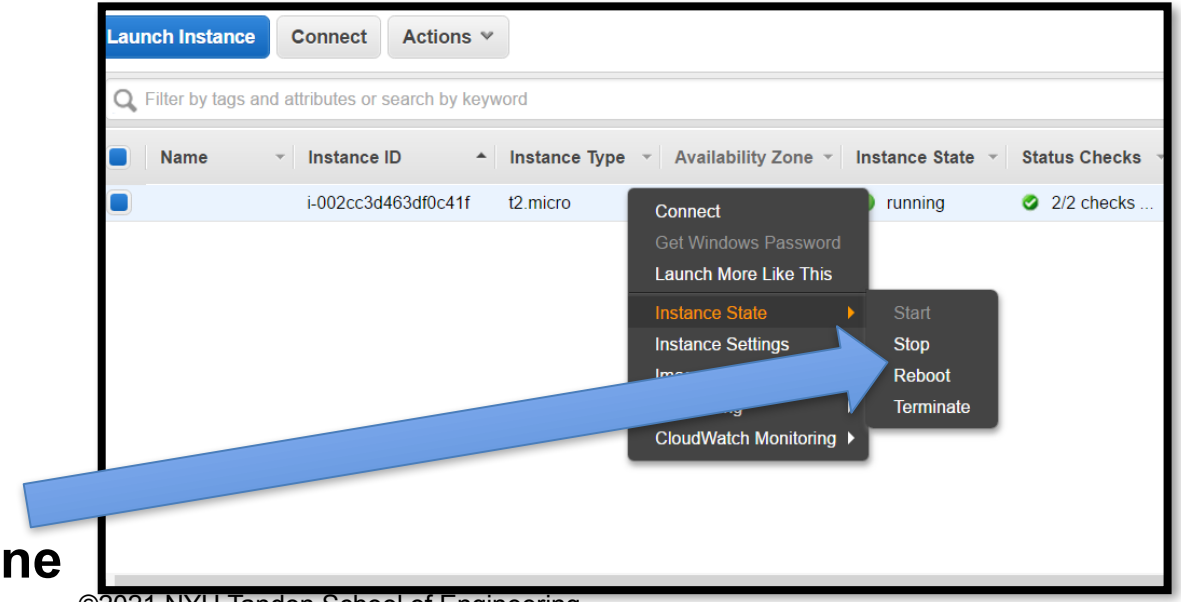


Go to Instances

AWS guide

- You can right-click and connect, or use an SSH tool like putty
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html?icmpid=docs_ec2_console
- Log in with your ec2-user username
- To get root
  - ? sudo su –





- Don't forget to stop your instance once done

Install Tools

- **Kali for AWS by default does not come with any tools**
- **Options:**
  - You will need to install each tool you need manually OR
  - Install a Kali Metapackage!
    - `$ sudo apt-get update`
    - `$ sudo apt -y install kali-linux-default`

- **All Metapackages:**
  - https://tools.kali.org/kali-metapackages
  - More info:
  - https://www.kali.org/news/major-metapackage-makeover/