

ACCA7033 Lab environment setup

Week 1

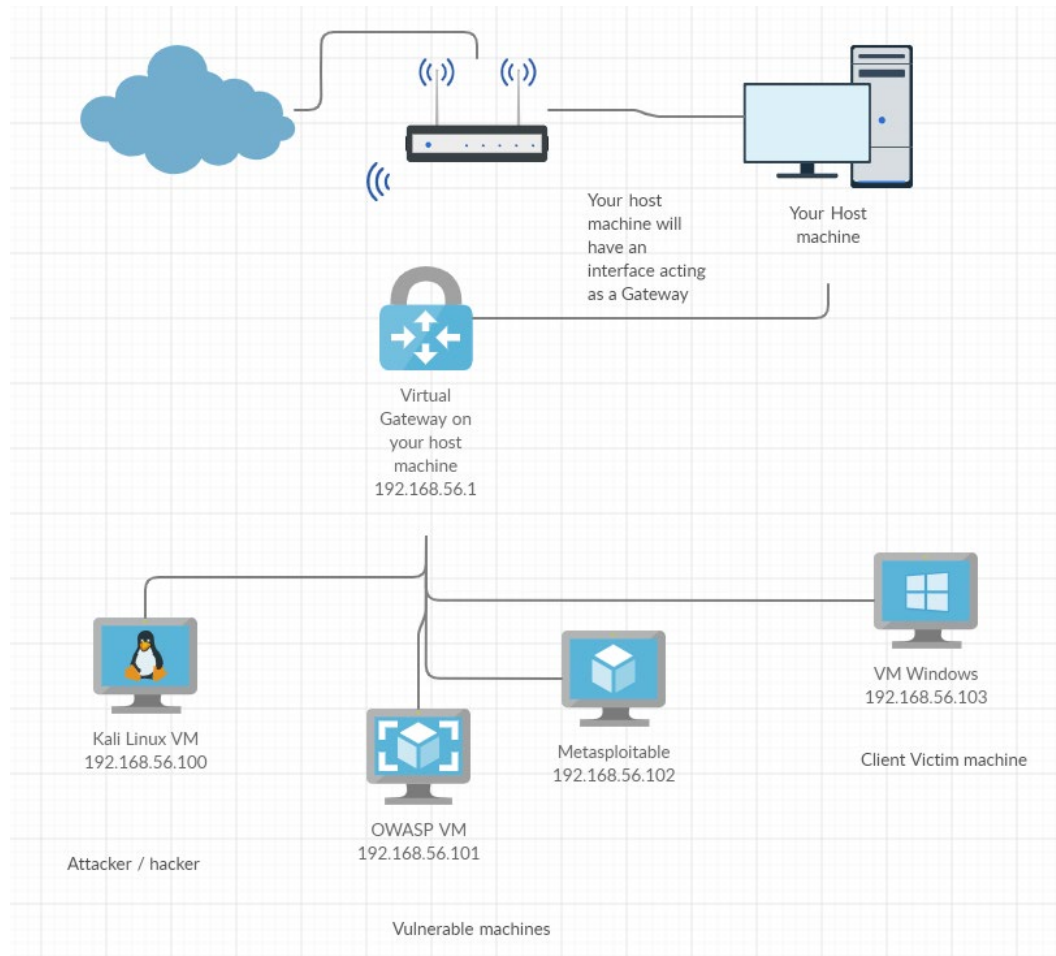


Figure 1: Ethical Hacking lab environment overview

1 Lab environment

For this course we will be using several virtual machines but the four essential now we will for sure use are below:

Kali, Metasploitable, OWASP, DVWA and Windows can be found in <https://www.osboxes.org/> and <https://www.vulnhub.com/>

Once your files are downloaded, you will need to install Virtual Box.

You will also need a virtual machines manager application. There are many you can use and you are free to use the one you are comfortable with. I usually use virtual box in my labs as they don't consume much resources. Other options such as VMware, hyperv, qemu, etc..

For this course we will be using Oracle Virtual box. You can download Oracle Virtual box from this [Virtual Box downloads link](#).

You need to make sure you are downloading the correct version - depending on your host Operating system

You do not need to download all virtual machines; some are not relevant for your module.

◀ For this module you will need the following VMs

- [Kali Linux 2019.3 and Kali Linux 2024.3](#)
- [Windows 7 Machine- Not needed until later in the module](#)
- [Metasploitable](#)
- [OWASP and DVWA](#)

◀ You will then need to import the three VMs you have downloaded. You can import in Virtual box by either click on the downloaded file directly and following instructions or by clicking on import to locate the file and import to virtual box as shown below.

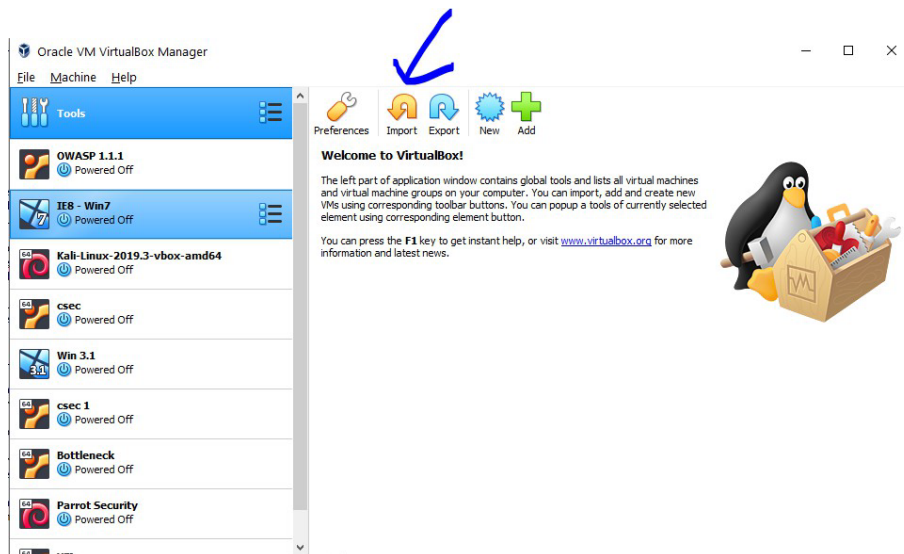


Figure 2: Import VMs into VirtualBox

1.1 Virtual machines setup

2 Network Setup

2.1 Internet Connected VM

Internet Connected Network

Sometimes, you need your Kali Linux VM to be connected to the Internet.

- < You never need to connect the Win7 machine or the OWASP machine to the Internet

The steps below will be the same for any VMs that you want it to be connected to the Internet (to the network your host machine is connected to)

- < Select the VM you need to change settings for and click on Settings. (Fig3)
- < Select Network (Fig4)
- < Choose in the drop-down menu of **Attached to** the option NAT. This is network Address Translation. This will give your virtual machine access to the network resources of your host machine. It will use the same IP address of your host machine to connect to the Internet. (Fig4)

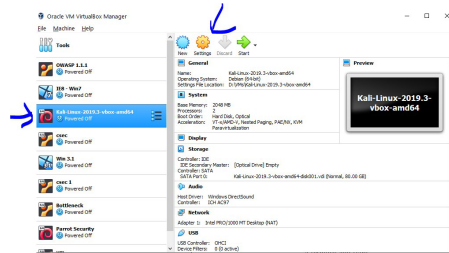


Figure 3: Choose Settings

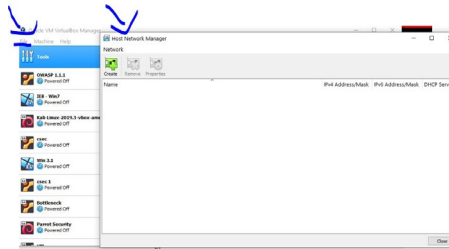


Figure 5: Enter into Host Network manager Setup window

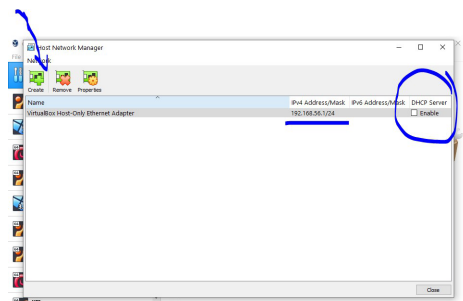


Figure 6: Create Network

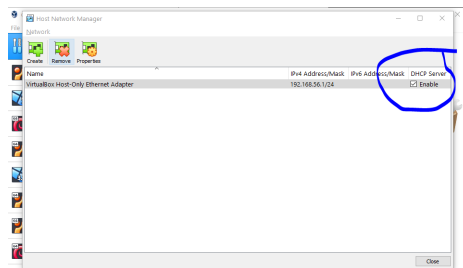


Figure 7: Enable DHCP

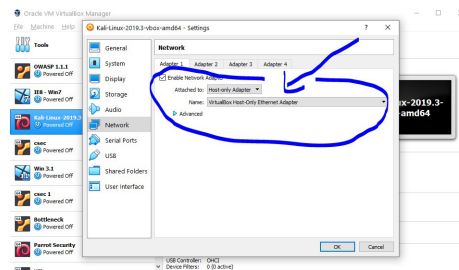


Figure 8: Host Only Adapter Settings

- To check your ip address, in any of those virtual machine devices you open a terminal and type:

- **ifconfig**

- In Windows you can open a command line Interface by clicking on start and typing cmd.

- **ipconfig**

`sudo dhclient eth1`

2.2.1 Manual IP Setup

- To check your ip address, in any of those virtual machine devices you open a terminal and type:

- **ifconfig**

- when we selected host only network we created a private network between our VMs that is completely isolated from the external world.

- We need to make sure both VMs are on the same network.

- **On Kali Linux machine terminal type:**

- **sudo ifconfig eth0 192.168.56.100 netmask 255.255.255.0** Fig9

- **On OWASP/Metasploitable machine terminal type:**

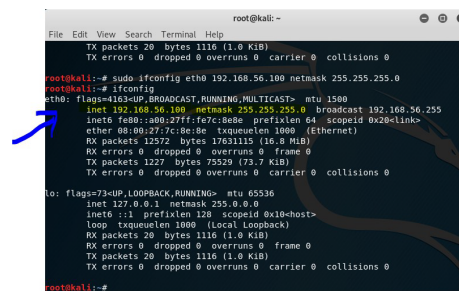
- **OWASP: sudo ifconfig eth0 192.168.56.101 netmask 255.255.255.0** Fig10

- **Metasploitable: sudo ifconfig eth0 192.168.56.102 netmask 255.255.255.0** Fig10

- **On Windows 7 machine**

- Go to control panel and select network and Internet as in Fig11

- Select Connect to a network as in Fig12
- Change Adapter Settings as in Fig13
- Select Local Area Network. Right click on it with your mouse pointer and select properties as in Fig14
- Select Internet Protocol Version 4 (TCP/IPv4) and click on properties as in Fig15
- Put the setting as shown below and shown in Fig16
 - * IP address : **192.168.56.103**
 - * Subnet Mask: **255.255.255.0**
 - * Default Gateway: **192.168.56.1** This Might be different for your machine. You will need to check the IP address given for the virtual box host only Network on your host machine



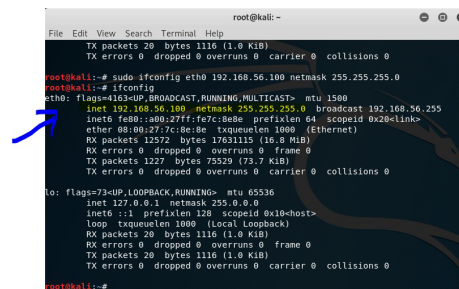
```

root@kali:~# sudo ifconfig eth0 192.168.56.103 netmask 255.255.255.0
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.56.103 netmask 255.255.255.0  broadcast 192.168.56.255
    inet6 fe80::a00:27ff:fe7c:8ede prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:7c:8e:de txqueuelen 1000 (Ethernet)
    RX packets 12572 bytes 17631115 (16.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1227 bytes 75529 (73.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
  
```

Figure 9: Manual Setup for Kali IP address



```

root@kali:~# sudo ifconfig eth0 192.168.56.103 netmask 255.255.255.0
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.56.103 netmask 255.255.255.0  broadcast 192.168.56.255
    inet6 fe80::a00:27ff:fe7c:8ede prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:7c:8e:de txqueuelen 1000 (Ethernet)
    RX packets 12572 bytes 17631115 (16.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1227 bytes 75529 (73.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
  
```

Figure 10: Manual Setup for OWASP IP address

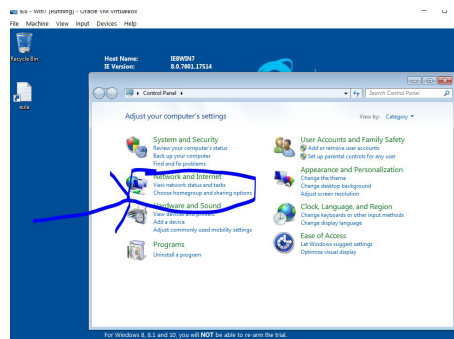


Figure 11: Windows: Control Panel

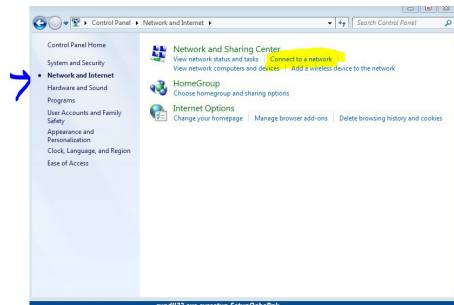


Figure 12: Windows: Network and Internet

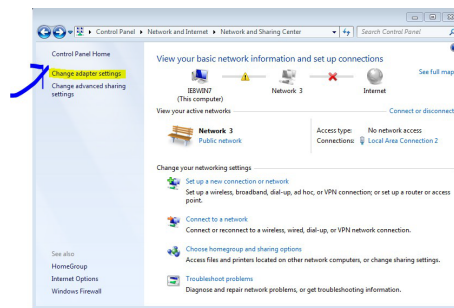


Figure 13: Windows: Change Adapter Settings

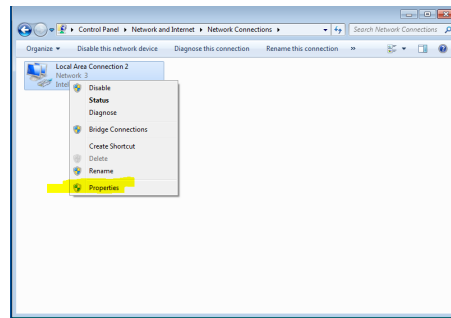


Figure 14: Properties

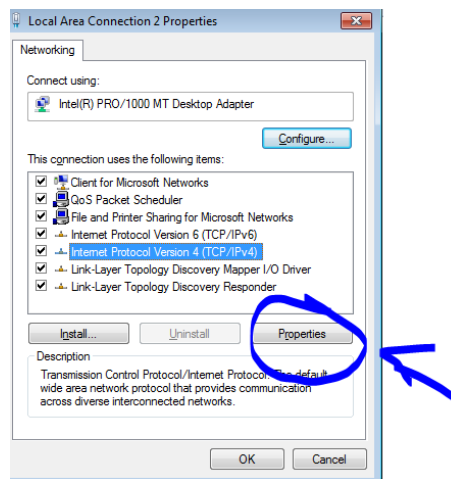


Figure 15: IPv4 properties

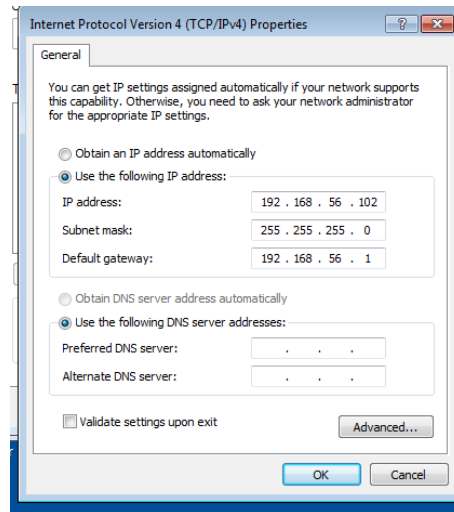


Figure 16: IP address, subnet and gateway

3 Test connectivity

- You can test connectivity on the terminal by using **ping** command to ping the vulnerable machine from kali or the other way around
 - To ping the vulnerable machine from kali **ping 192.1268.56.100**
- when we selected host only network we created a private network between our VMs that is completely isolated from the external world.
- **Remember for any two devices to communicate. they need to be on the same network.**
- We need to make sure both VMs are on the same network with the host machine only.
- On the Vulnerable machine terminal type:
 - **sudo ifconfig eth0 192.168.56.100 netmask 255.255.255.0**
- On Kali Linux machine terminal type:
 - **sudo ifconfig eth0 192.168.56.101 netmask 255.255.255.0**
- You also test connectivity between kali Linux and the vulnerable machine by opening a browser on the kali Linux machine and entering in the address bar the ip address of the vulnerable machine.
- You should see the OWASP Broken Web Applications Project page as shown below

- If connectivity test fails between any of the Linux machines and the Windows 7 machine. Switch of the firewall as the security of the victim machine is out of the scope of this module.

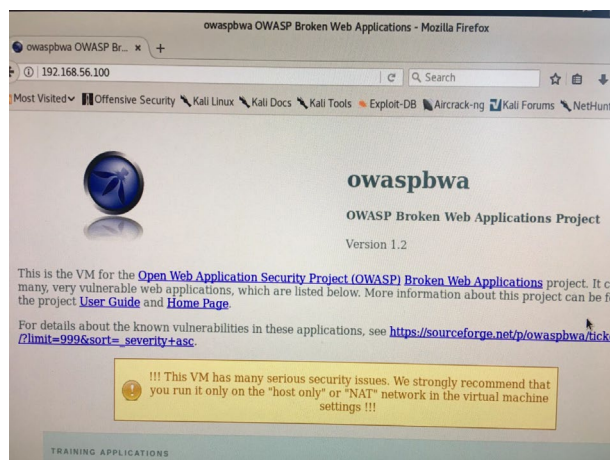


Figure 17: OWASP page

4 Update Kali Linux and install app

For our labs, we will need a browser attachment called **OWASP mantra**

- **Update repositories for Linux** by typing
 - `sudo apt-get update`
- **Install OWASP mantra** by typing
 - `sudo apt-get install OWASP-mantra-f`

Access OWASP Mantra

- To access OWASP Mantra < click on **Applications < 03- Web Application Analysis < Web Vulnerability Scanners**

git

- Install git < open a terminal and type `sudo apt-get install git` < **Web Vulnerability Scanners**

5 Getting to know web applications on a vulnerable VM

OWASP-bwa contains many web applications, intentionally made vulnerable to the most common attacks. Some of them are focused on the practice of some specific technique while others try to replicate real-world applications that happen to have vulnerabilities.

1. With OWASP VM running, open your Kali Linux host's web browser and go to <http://192.168.56.101>. You will see a list of all applications the server contains as shown in Fig5.
2. For **Damn vulnerable Web Application**. Use username **admin** and password **admin**. We can see a menu on the left; this menu contains links to all the vulnerabilities that we can practice in this application: Brute Force, Command Execution, SQL Injection, and so on.
3. **OWASP WebGoat.NET**. This is a .NET application where we will be able to practice file and code injection attacks, cross-site scripting, and encryption vulnerabilities. It also has a WebGoat Coins Customer Portal that simulates a shopping application and can be used to practice not only the exploitation of vulnerabilities but also their identification

The applications in the home page are organized in the following six groups:

- ◀ **Training applications:** These are the ones that have sections dedicated to practice-specific vulnerabilities or attack techniques; some of them include tutorials, explanations, or other kind of guidance.
- ◀ **Realistic, intentionally vulnerable applications:** Applications that act as real-world applications (stores, blogs, and social networks) and are intentionally left vulnerable by their developers for the sake of training.
- ◀ **Old (vulnerable) versions of real applications:** Old versions of real applications, such as WordPress and Joomla are known to have exploitable vulnerabilities; these are useful to test our vulnerability identification skills.
- ◀ **Applications for testing tools:** The applications in this group can be used as a benchmark for automated vulnerability scanners.
- ◀ **Demonstration pages / small applications:** These are small applications that have only one or a few vulnerabilities, for demonstration purposes only. OWASP demonstration application: OWASP AppSensor is an interesting application, it simulates a social network and could have some vulnerabilities in it. But it will log any attack attempts, which is useful when trying to learn; for example, how to bypass some security devices such as a web application firewall.

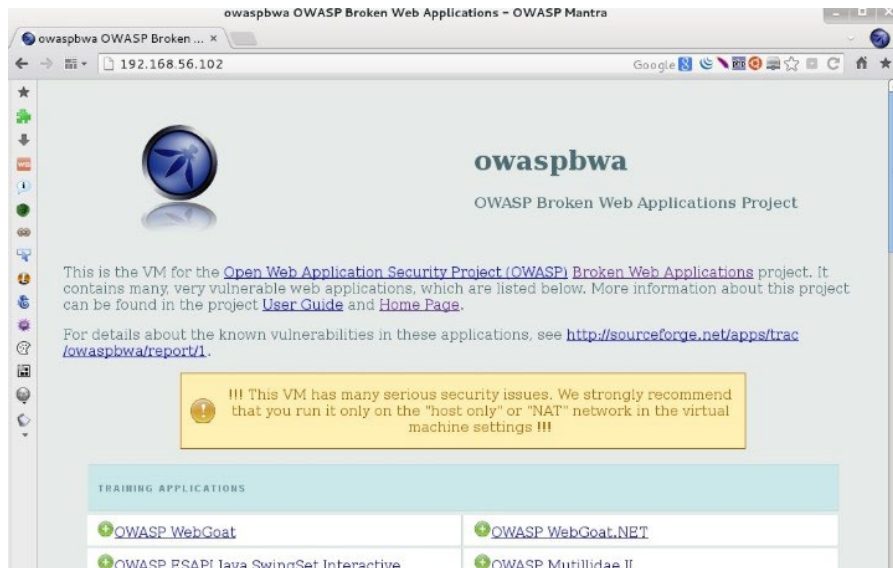


Figure 18: OWASP Web Interface

6 Setting up python 3 in Linux

◀ Install python

- **sudo apt-get install python2.7**
- Let us remove all other dependencies that we are not using. **sudo apt-get autoremove**

7 Problems that you can possibly face

We faced some problems in the class. I want to avoid having those problems every week as it will take away from our lab time.

1. on VMware, make sure your virtual network is connected as in (virtually connected)
2. on VBox, you need to create a virtual box network interface first
3. If you cannot see any virtual interface on your computer and you are using VMware type **sudo systemctl restart VMware**.
4. On kali Linux, changes you made in your network interface were not taking effects until the network manager service was restarted by using **sudo service network-manager restart**

5. In some machines, you need to change the USB setting for the VM to USB 1.1 as shown in fig below. This applies for any machines that throw the USB error.

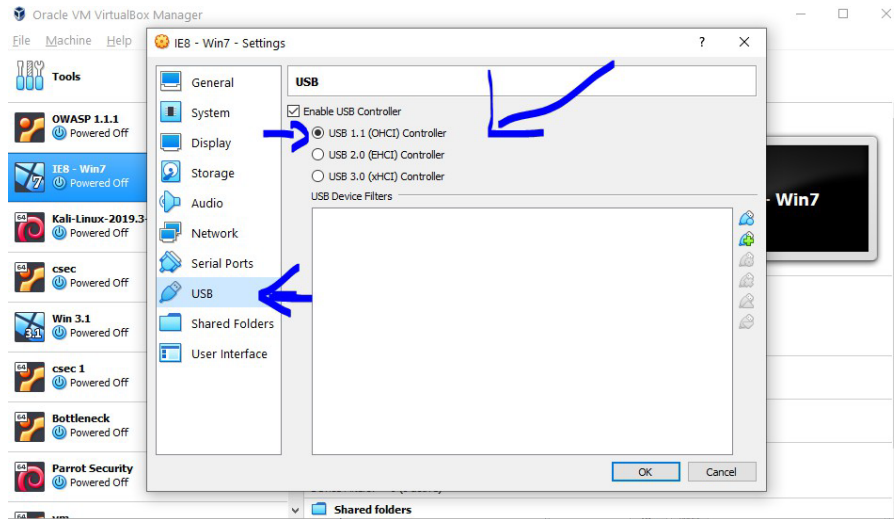


Figure 19: USB error