Why do I need a pen test lab?

- Hacking and or scanning machines without consent is against the law in most countries
- To become an effective penetration tester or ethical hacker you need to practice to enhance your skills
- Freedom to install, run, and configure any tool you like

Requirements

- Hard Disk - 50GB of disk space or more depending on the number of guest operating systems you plan on installing.
- CPU - I recommend the latest technology but any of the I3/I5/I7 families are ok. The more processing power you have the better
- Memory - I recommend 8GB or 16GB. Memory is critical. The more memory you have the more virtual systems you will be able to have running at one time
- Virtualization software – I recommend using open source software to start using either VirtualBox or VMPlayer. Eventually you might want to pay for the commercial software such as VMworkstation of if you have a Mac VMfusion

Virtual Machine Downloads

- **Kali Linux 2 -Pentesting Environment**
  - Osboxes.org
  - https://www.offensive-security.com/kali-linux-vmware-arm-image-download/
- **Metasploitable 2 – Vulnerable Machine**
  - http://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- **Bee-Box – Vulnerable Machine**
  - http://sourceforge.net/projects/bwapp/files/bee-box/bee-box_v1.6.7z/download
- **OWASP Brocken Web Applications Project – Vulnerable Machine**
  - http://sourceforge.net/projects/owaspbwa/files/

Virtualization Software

- For this class I will be using **VirtualBox**
    - https://www.virtualbox.org/wiki/Downloads
    - Install the software based on your host operating system
        - Windows, OSX, Linux, or Solaris

Folder Structure

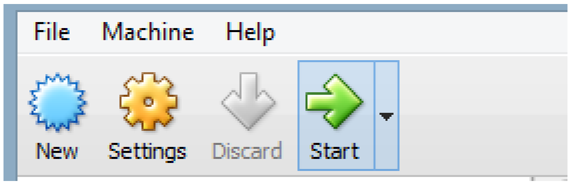
- I recommend creating 2 folders for this work
    - A folder for the compressed files so that if need be you can recreate the vms in case you end up with a corrupted VM
    - A folder for the uncompressed Virtual Machines

Extracting Files

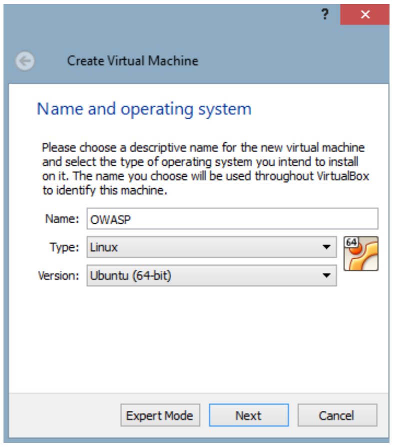
- I recommend downloading 7-zip if you don't already have winzip. 7-zip is open source software which can decompress a large number of compressed file types.
    - http://www.7-zip.org/

Creating Virtual Machines

- Open Virtual Box
- Click New



- Enter the Name and Operating System and Click Next



Name and operating system

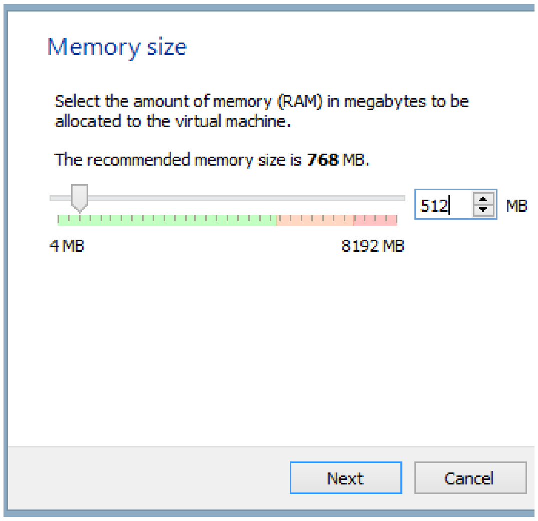
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: OWASP

Type: Linux

Version: Ubuntu (64-bit)

- Change the memory size to 512



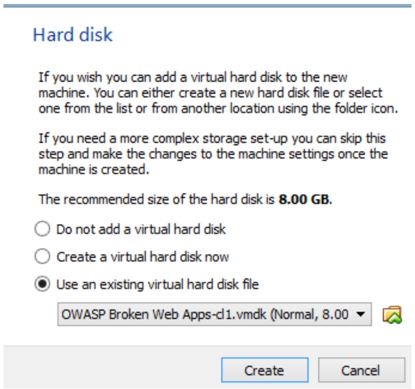
Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **768** MB.

512 MB

- Use and existing virtual hard disk



Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

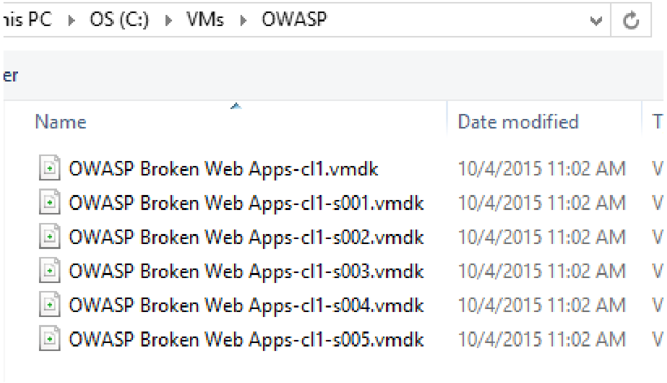
○ Do not add a virtual hard disk

○ Create a virtual hard disk now

● Use an existing virtual hard disk file

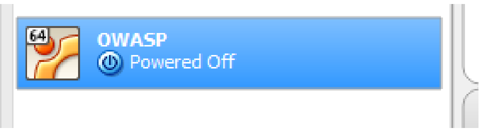
OWASP Broken Web Apps-cl1.vmdk (Normal, 8.00

- Click on the folder icon above cancel and select the folder and file that you want to use. Click Open. Then click Create. Select the first file cl1.vmdk…

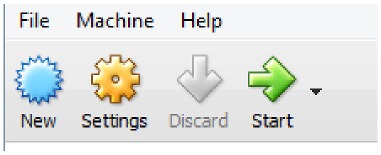


Name	Date modified	T
OWASP Broken Web Apps-cl1.vmdk	10/4/2015 11:02 AM	V
OWASP Broken Web Apps-cl1-s001.vmdk	10/4/2015 11:02 AM	V
OWASP Broken Web Apps-cl1-s002.vmdk	10/4/2015 11:02 AM	V
OWASP Broken Web Apps-cl1-s003.vmdk	10/4/2015 11:02 AM	V
OWASP Broken Web Apps-cl1-s004.vmdk	10/4/2015 11:02 AM	V
OWASP Broken Web Apps-cl1-s005.vmdk	10/4/2015 11:02 AM	V

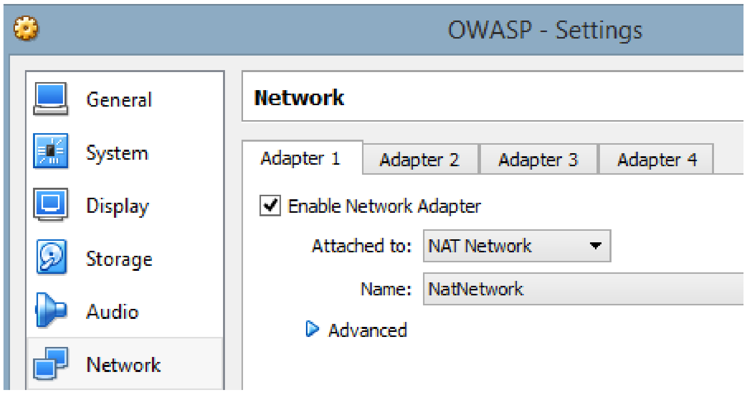
- Now you will see your virtual machine on the vm list’



- Click on Settings



- Click on Network. Change Attached to to Nat Network. Name NatNetwork and click OK

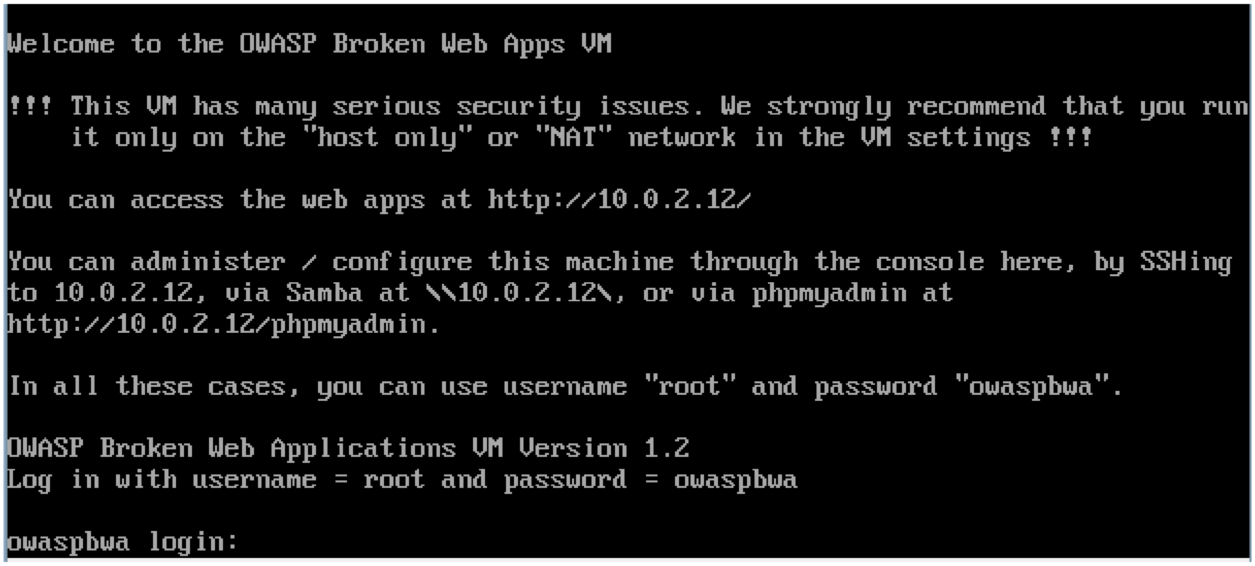


☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork

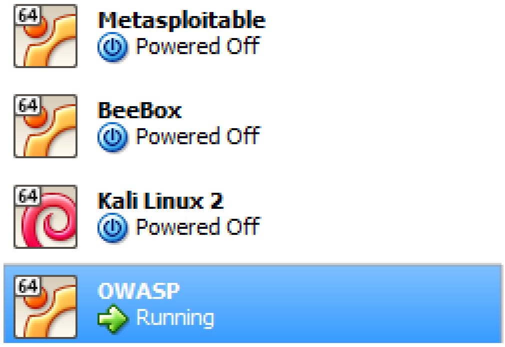
- Click on Start
  - Wait for the machine to run. You will then be at the login screen. Enter the password of root and the password of owaspbwa



```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://10.0.2.12/

You can administer / configure this machine through the console here, by SSHing
to 10.0.2.12, via Samba at \\10.0.2.12\, or via phpmyadmin at
http://10.0.2.12/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login:
```

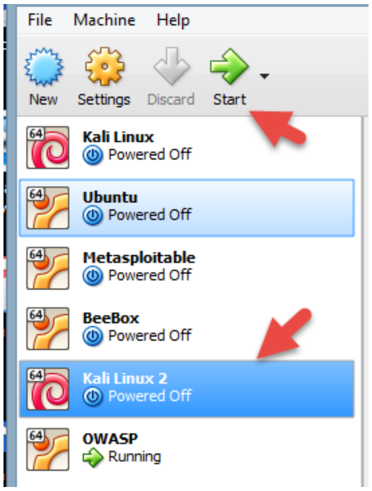
- You will now be logged in as root and be at the # prompt. This is all you need to do with this VM. Write down the ip address as in this case it is 10.0.2.12 so you can use it later.

Create the other VMS just as you did with this one. When you are done you should have a virtual machine list that looks like this:

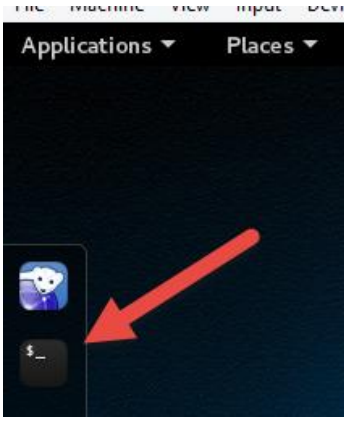


Kali Linux

- Video 1 https://www.youtube.com/watch?v=HQYcgvISi9Y
- Video 2 https://www.offensive-security.com/kali-linux-vmware-arm-image-download/
- Start Kali Linux VM

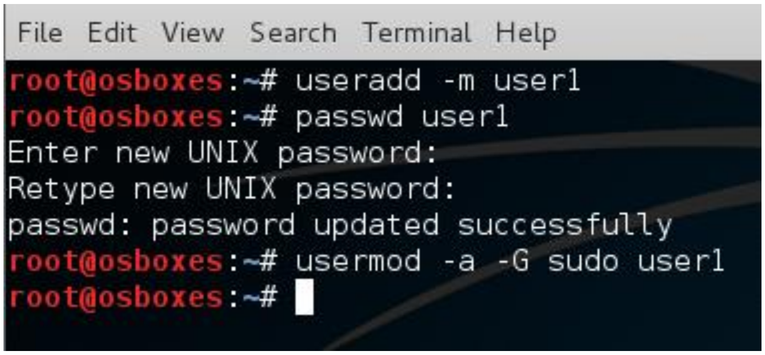


- Login with the username of **root**
- Enter the password of **toor** if you downloaded the Vm from offensive security
- Enter the password of **osboxes.org** if you downloaded the VM from osboxes.org
- Open up a terminal session



- Create a new user called user1
  - Type **useradd –m user1**
- Create a password for user1
  - Type **passwd user1**
  - Type **root**
  - Retype **root**

- Add user1 to the sudo group
  - Type **usermod –a –G sudo user1**



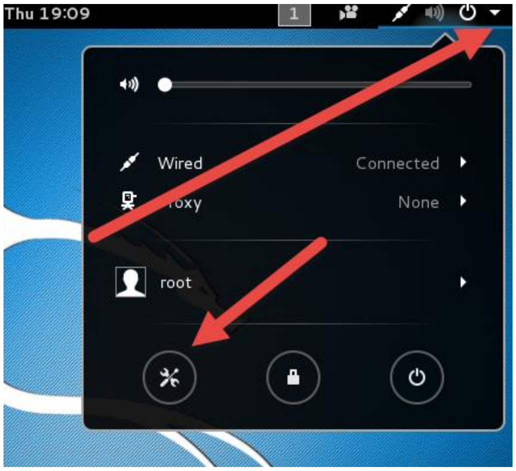
```
root@osboxes:~# useradd -m user1
root@osboxes:~# passwd user1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@osboxes:~# usermod -a -G sudo user1
root@osboxes:~#
```

Update Kali Distribution

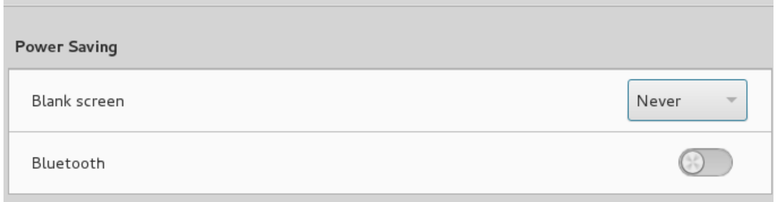
- Now let’s **update our Kali Distribution**
  - Type **apt-get update**
  - Once complete and you are back at the # prompt
  - Type **apt-get dist-upgrade**
  - Type **y** and hit **enter**
  - When done type **exit**

Power Settings

- Now let’s **turn off power saving**
- Click on the down arrow in the top right of screen then click on settings



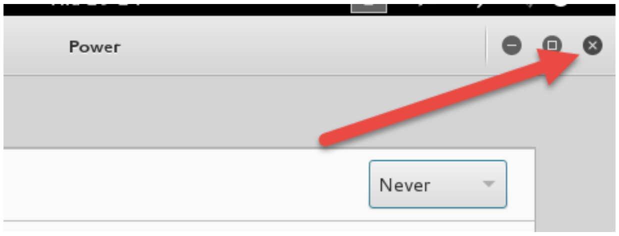
- Click on **Power**
- Change Blank screen to **Never**


Power Saving

Blank screen Never

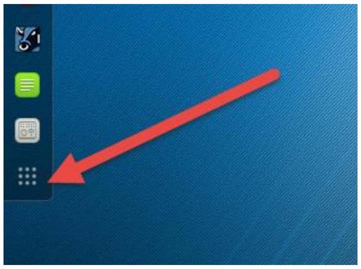
Bluetooth

- Close out of Power Settings

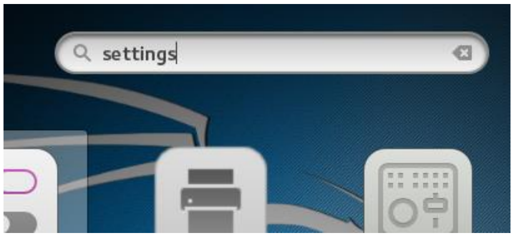


Privacy Settings

- Change Privacy Settings
- Click on Show Applications

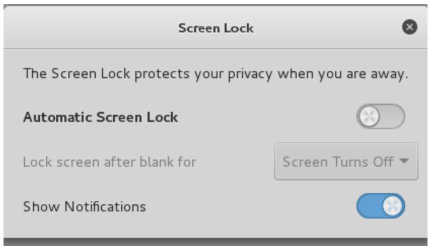


- Type **settings** in the search bar and hit **enter**



settings

- Click **Privacy**
- Change Screen Lock by turning off **Automatic Screen Lock**



Screen Lock

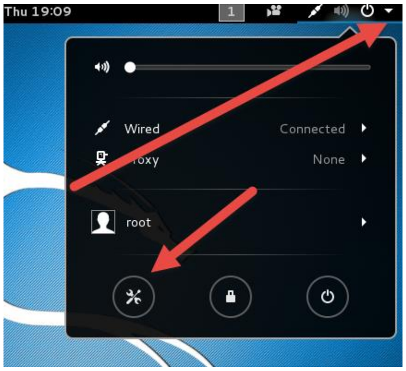
The Screen Lock protects your privacy when you are away.

Automatic Screen Lock ○

Lock screen after blank for: Screen Turns Off

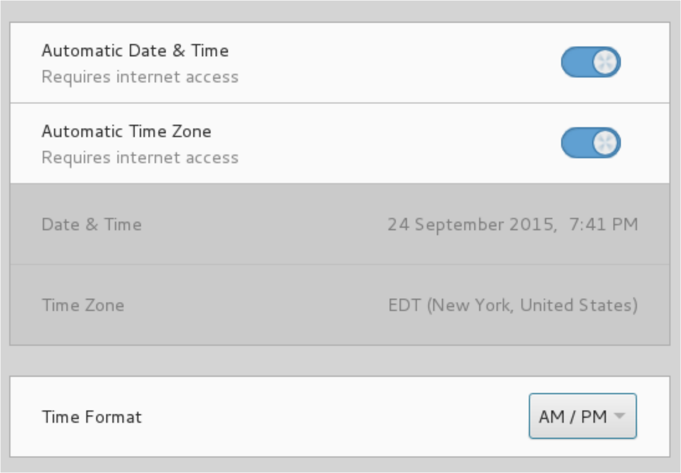
Show Notifications ●

  - Close out of screenlock
- Now let's set our system data and time. Click on **settings** again



Date & Time

- Click on **Date & Time**
  - Turn on Automatic Date & Time
  - Turn on Automatic Time Zone
  - Change Time Format to AM/PM



Automatic Date & Time
Requires internet access

Automatic Time Zone
Requires internet access

Date & Time 24 September 2015, 7:41 PM

Time Zone EDT (New York, United States)

Time Format AM / PM

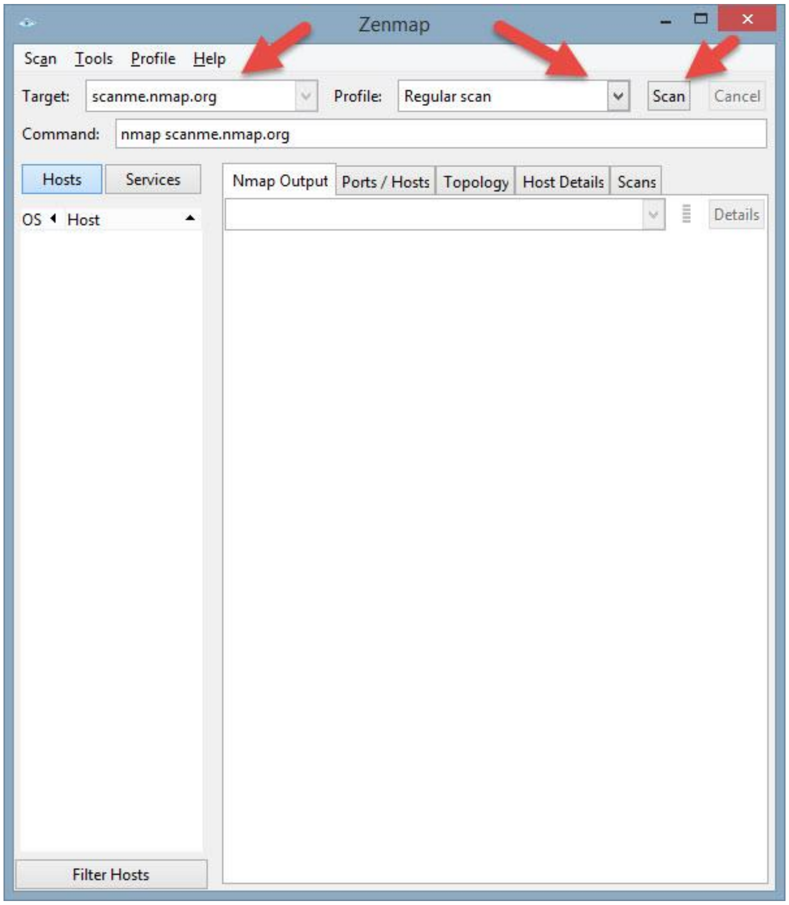
- Close out of Date & Time

Nmap

- Open a terminal session
- Test your network connectivity and make sure nmap is working
- Type **nmap scanme.nmap.org**
- Review the results to see the open ports and services found

Zenmap

- At the command line type Zenmap
- Enter scanme.nmap.org as the target
- Select the profile of Regular scan and hit the scan button



Target: scanme.nmap.org

Profile: Regular scan

Command: nmap scanme.nmap.org

Nmap Scans

Run the following scans against scanme.nmap.org

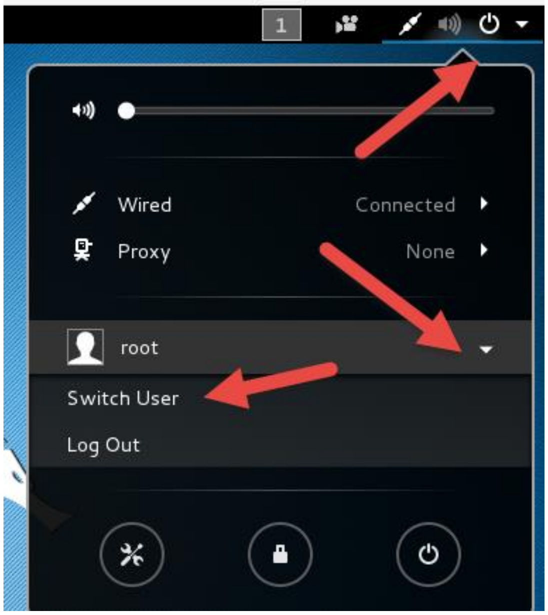
- **Nmap –sn scanme.nmap.org** (just a ping)
- **Nmap –Pn scanme.nmap.org** (without a ping stealthy)
- **Nmap –A scanme.nmap.org** (aggressive scan)
- **Nmap –p 80 scanme.nmap.org –** Nmap can select what ports to scan by simply adding –p port,port2,port 3… In this case we will only scan port 80.
- **Nmap –p- scanme.nmap.org** – Scans all ports from port 1-65535. It can also be accomplished by **nmap –p 1-65535 scanme.nmap.org**.

Zenmap Scans

Enter the target of scanme.nmap.org and select the following profiles and hit the scan button. Look at the commands.

- **Regular Scan**
- **Quick traceroute**
- **Quick scan**
- **Intense scan, all TCP ports**

- Switch user to user1

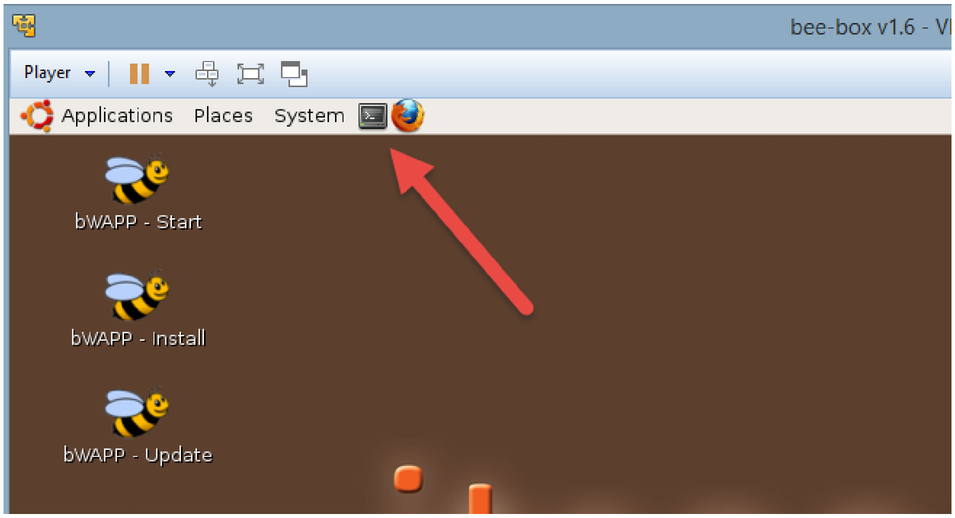


- Login with the username of **user1**
- Enter the password of **root**
- Open up a terminal session and notice that now you have a $ prompt as opposed to a # prompt. You are no longer logged in as root so the # is replaced with a $.
- Now when you run your nmap commands you are going to have to enter sudo before the nmap command

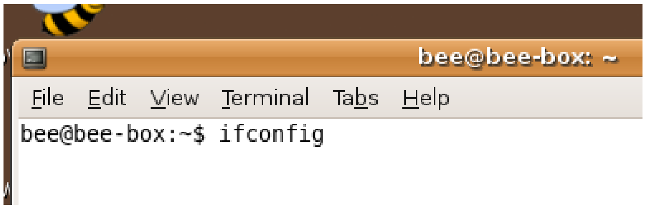
Scanning Vulnerable Virtual Machines

Bee-Box

- Start Bee-Box
- Open up a terminal session

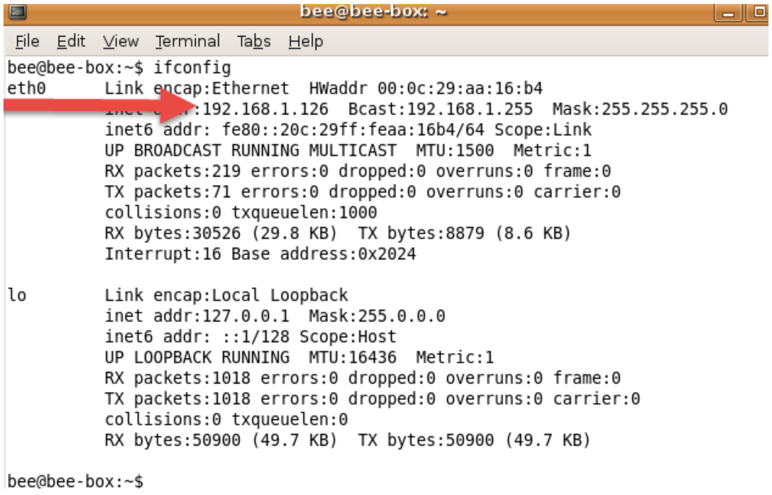


- Type ifconfig and hit enter



```
bee@bee-box:~$ ifconfig
```

- You should get an IP address



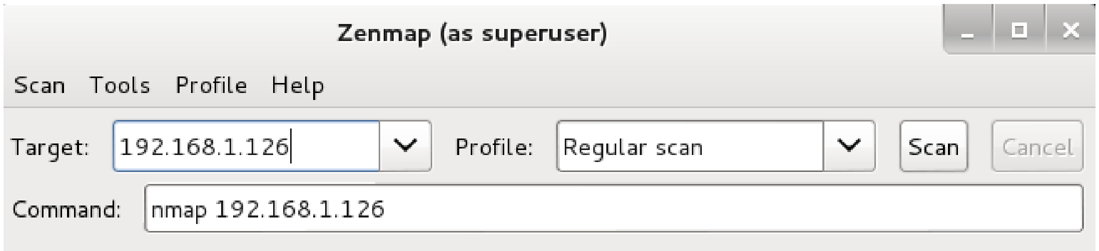
```
bee@bee-box:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:aa:16:b4
          inet addr:192.168.1.126  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feaa:16b4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:219 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30526 (29.8 KB)  TX bytes:8879 (8.6 KB)
          Interrupt:16 Base address:0x2024

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:1018 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1018 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50900 (49.7 KB)  TX bytes:50900 (49.7 KB)

bee@bee-box:~$
```

- Write down the ip address as you are going to use it throughout the nmap and Zenmap exercises. Mine is 192.168.1.126. Yours will be different
- Go back to Kali Linux and open up a terminal session
- Type **sudo nmap –sn x.x.x.x** (ip address from bee-box)
- Enter the password of user1 - **root**
- Type **sudo Nmap ip address**
- Type **sudo nmap –Pn IP address**
- Type **sudo nmap –F IP Address** This scan will scan the top 100 ports.
- Type **sudo Nmap --top-ports 10 ip address** This will only scan the top 10 ports.

- Type **sudo nmap –open ip address** This scan will only display the open ports
- Type **sudo nmap –p 80 ip address** This will only scan port 80.
- Type **sudo nmap –p 80,445 IP Address** This will only scan ports 80 and 445.
- Type **sudo nmap –p 20-500** This will scan ports 20 through 600.
- Type **sudo nmap –p- ip** address This will scan all the TCP ports 1-65535. You can also achieve the same thing by typing **sudo nmap –p 1-65535 ip address**
- Type **sudo nmap –sV ip address** This will scan the top 1000 ports and provide details about the services.
- Type **sudo nmap – O ip address** in order to scan the top 1000 ports but also scan for the operating system. Nmap has a database of operating systems it uses to compare to the system…
- Type **sudo nmap – A ip address** in order to perform an aggressive scan which includes, open ports, OS, Services, traceroute, and mac address. This is not a stealthy scan by any means… It will take much longer than any of the other scans.
- Type **sudo nmap –T5 ip address** to run an insane fast scan. The other options are -T4 (aggressive), -T3 (normal), -T2 (polite), -T1 (Sneaky), -T0 (paranoid)

Zenmap

- Enter the target IP address, Profile select regular scan, and hit the scan button



Target: 192.168.1.126

Profile: Regular scan

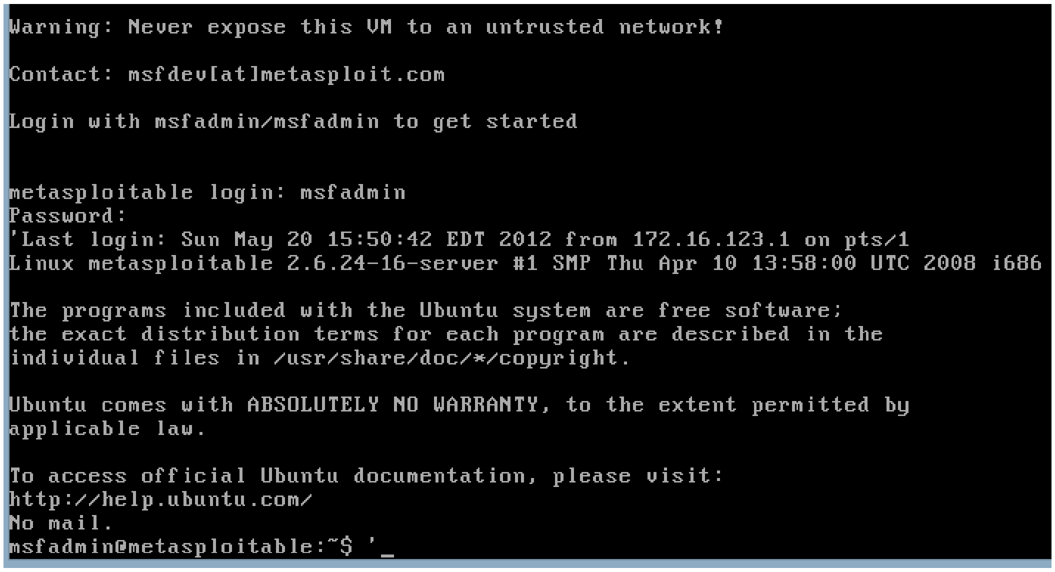
Command: nmap 192.168.1.126

- Now let’s perform a **Quick scan** by changing the profile to **quick scan** and hitting the **scan button**

Metasploitable

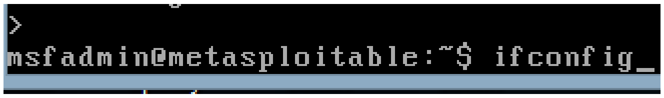
Metasploitable

- Start Metasploitable
- Login as msfadmin/msfadmin



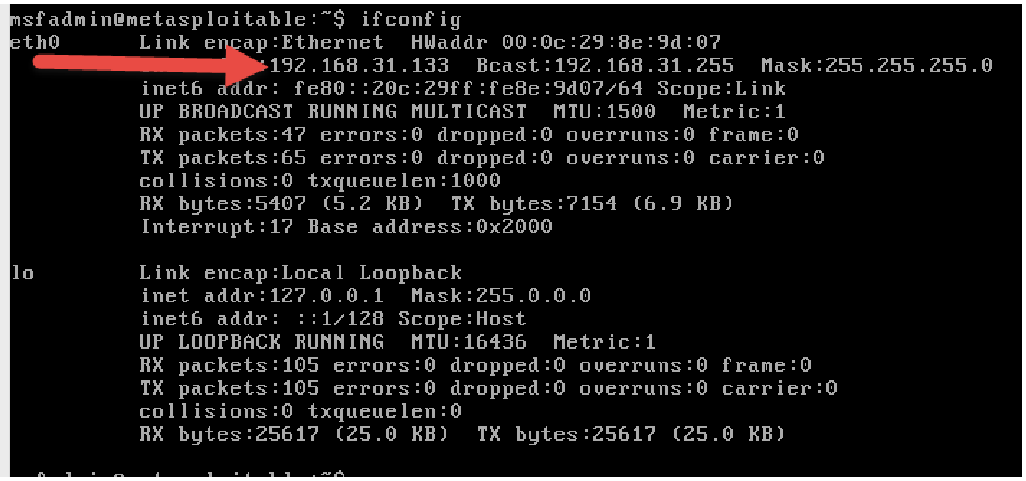
```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
'Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ '_
```

- Type **Ifconfig**



```
>
msfadmin@metasploitable:~$ ifconfig_
```

- You should get an IP address



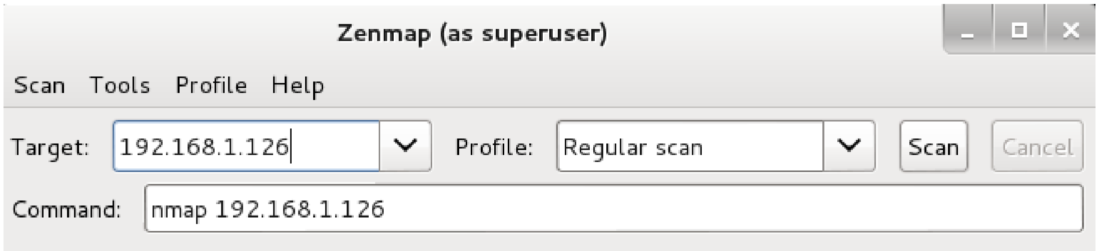
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:8e:9d:07
                    192.168.31.133  Bcast:192.168.31.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe8e:9d07/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5407 (5.2 KB)  TX bytes:7154 (6.9 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:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25617 (25.0 KB)  TX bytes:25617 (25.0 KB)
```

- Write down the ip address as you are going to use it throughout the nmap and Zenmap exercises. Mine is 192.168.31.133. Yours will be different
- Go back to Kali Linux and open up a terminal session
- Type **sudo nmap –sn x.x.x.x** (ip address from metasploitable)
- Type **sudo Nmap ip address**
- Type **sudo nmap –Pn IP address**
- Type **sudo nmap –F IP Address** This scan will scan the top 100 ports.
- Type **sudo Nmap --top-ports 10 ip address** This will only scan the top 10 ports.
- Type **sudo nmap –open ip address** This scan will only display the open ports
- Type **sudo nmap –p 80 ip address** This will only scan port 80.

- Type **sudo nmap –p 80,445 IP Address** This will only scan ports 80 and 445.
- Type **sudo nmap –p 20-500** This will scan ports 20 through 600.
- Type **sudo nmap –p- ip** address This will scan all the TCP ports 1-65535. You can also achieve the same thing by typing **sudo nmap –p 1-65535 ip address**
- Type **sudo nmap –sV ip address** This will scan the top 1000 ports and provide details about the services.
- Type **sudo nmap – O ip address** in order to scan the top 1000 ports but also scan for the operating system. Nmap has a database of operating systems it uses to compare to the system…
- Type **sudo nmap – A ip address** in order to perform an aggressive scan which includes, open ports, OS, Services, traceroute, and mac address. This is not a stealthy scan by any means… It will take much longer than any of the other scans.
- Type **sudo nmap –T5 ip address** to run an insane fast scan. The other options are -T4 (aggressive), -T3 (normal), -T2 (polite), -T1 (Sneaky), -T0 (paranoid)

Zenmap

- Enter the tar
- Enter the target IP address, Profile select regular scan, and hit the scan button



Target: 192.168.1.126

Profile: Regular scan

Command: nmap 192.168.1.126

- Now let’s perform a **Quick scan** by changing the profile to **quick scan** and hitting the **scan button**

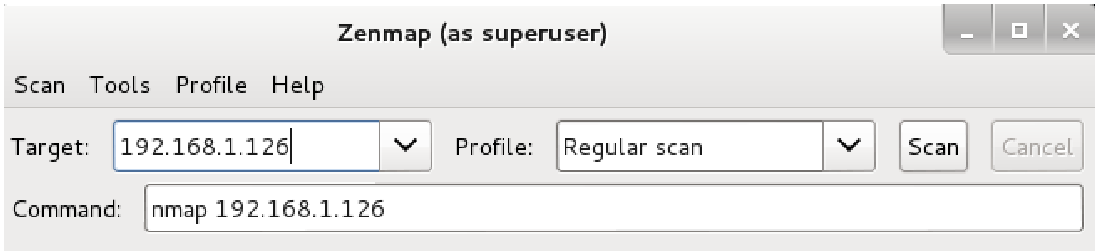
OWASP

- Your OWASP machine should already be running. You logged in s root with a password of owaspbwa. You should have already written down the ipaddress from earlier
- Go back to Kali Linux and open up a terminal session
- Type **sudo nmap –sn x.x.x.x** (ip address from Owasp)
- Type **sudo Nmap ip address**
- Type **sudo nmap –Pn IP address**
- Type **sudo nmap –F IP Address** This scan will scan the top 100 ports.
- Type **sudo Nmap --top-ports 10 ip address** This will only scan the top 10 ports.

- Type **sudo nmap –open ip address** This scan will only display the open ports
- Type **sudo nmap –p 80 ip address** This will only scan port 80.
- Type **sudo nmap –p 80,445 IP Address** This will only scan ports 80 and 445.
- Type **sudo nmap –p 20-500** This will scan ports 20 through 600.
- Type **sudo nmap –p- ip** address This will scan all the TCP ports 1-65535. You can also achieve the same thing by typing **sudo nmap –p 1-65535 ip address**
- Type **sudo nmap –sV ip address** This will scan the top 1000 ports and provide details about the services.
- Type **sudo nmap – O ip address** in order to scan the top 1000 ports but also scan for the operating system. Nmap has a database of operating systems it uses to compare to the system…
- Type **sudo nmap – A ip address** in order to perform an aggressive scan which includes, open ports, OS, Services, traceroute, and mac address. This is not a stealthy scan by any means… It will take much longer than any of the other scans.
- Type **sudo nmap –T5 ip address** to run an insane fast scan. The other options are -T4 (aggressive), -T3 (normal), -T2 (polite), -T1 (Sneaky), -T0 (paranoid)

Zenmap

- Enter the tar
- Enter the target IP address, Profile select regular scan, and hit the scan button



Target: 192.168.1.126 Profile: Regular scan

Command: nmap 192.168.1.126

- Now let’s perform a **Quick scan** by changing the profile to **quick scan** and hitting the **scan button**

Scanning all Vulnerable VMs at once

- Type **sudo nmap –sn ip 192.168.31.133 192.168.1.126, 192.168.1.135 (use your ip addresses not mine)**
- Type **sudo nmap ip 192.168.31.133 192.168.1.126, 192.168.1.135 (use your ip addresses not mine)**
- Type **sudo nmap –F 192.168.31.133 192.168.1.126 192.168.1.135 (use your ip addresses not mine)**
- Type **sudo nmap --top-ports 10 192.168.31.133 192.168.1.126 (use your ip addresses not mine)**

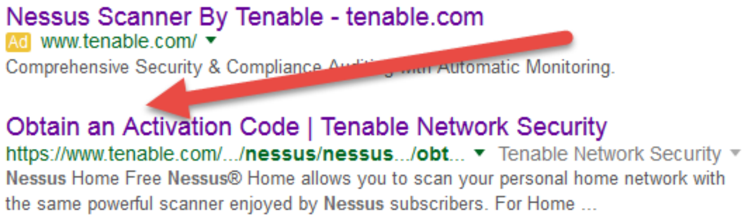
Zenmap Scanning of Vulnerable VMs

- Type sudo zenmap at the command line
- Enter the ip address of bee-box as the target. Select regular scan and hit the scan button
- Enter the ip address of metasploitable as the target. Select regular scan and hit the scan button
- Enter the ip address of OWASP as the target. Select regular scan and hit the scan button
- Exit Zenmap

Nessus

Activation Code

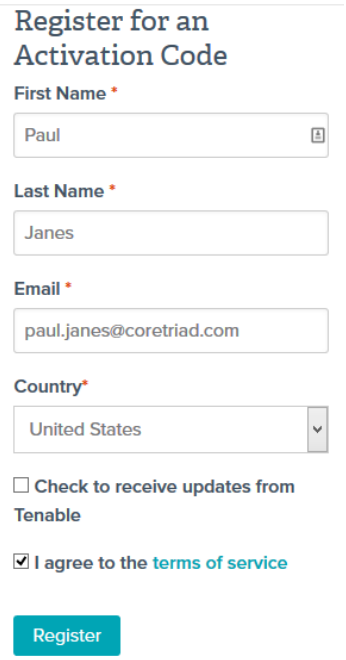
- Open google and search for **nessus obtain an activation code**
- Click on **Obtain an Activation Code | Tenable Network Security**



Nessus Scanner By Tenable - tenable.com
Ad www.tenable.com/ ▾
Comprehensive Security & Compliance Auditing with Automatic Monitoring.

Obtain an Activation Code | Tenable Network Security
https://www.tenable.com/.../**nessus/nessus**.../**obt**... ▾ Tenable Network Security ▾
Nessus Home Free **Nessus**® Home allows you to scan your personal home network with the same powerful scanner enjoyed by **Nessus** subscribers. For Home ...

- Under Nessus Home Click **Register Now**
- Enter your information and hit **Registe**r



Register for an Activation Code

First Name *

Paul

Last Name *

Janes

Email *

paul.janes@coretriad.com

Country*

United States

□ Check to receive updates from Tenable

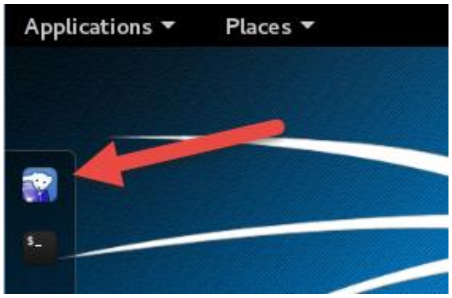
☑ I agree to the terms of service

Register

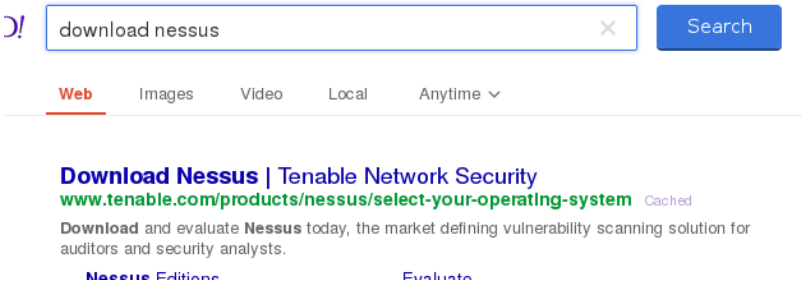
- Wait a few minutes and check your email

Nessus Download

- Open up the Iceweasel web browser

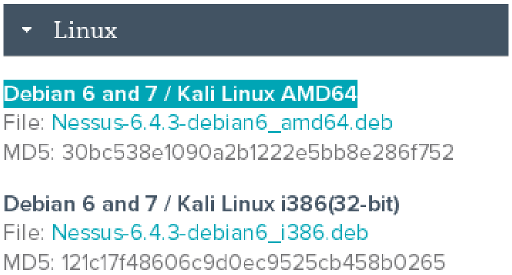


- Search for **download nessus** and hit search



Download Nessus | Tenable Network Security
www.tenable.com/products/nessus/select-your-operating-system Cached
Download and evaluate **Nessus** today, the market defining vulnerability scanning solution for auditors and security analysts.

- Click **Download Nessus**
- Scroll down and **Download Nessus Home**
- Select your Operation System – **Linux**

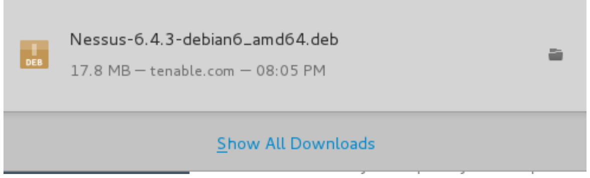


Linux

Debian 6 and 7 / Kali Linux AMD64
File: Nessus-6.4.3-debian6_amd64.deb
MD5: 30bc538e1090a2b1222e5bb8e286f752

Debian 6 and 7 / Kali Linux i386(32-bit)
File: Nessus-6.4.3-debian6_i386.deb
MD5: 121c17f48606c9d0ec9525cb458b0265

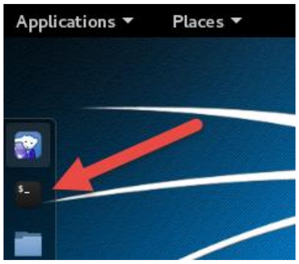
- Select the file for your operating system **32 or 64 bit**.
- Agree to the Subscription Agreement
- Click on Save File
- When the file has downloaded you should see the following:



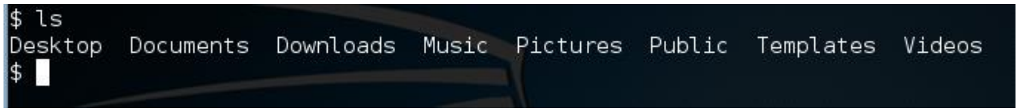
Nessus-6.4.3-debian6_amd64.deb
17.8 MB — tenable.com — 08:05 PM

Nessus Installation

- Close your browser and open a terminal session

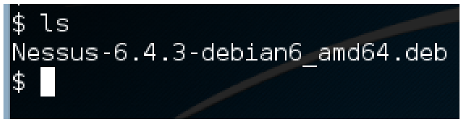


- Type **ls**



```
$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
$ 
```

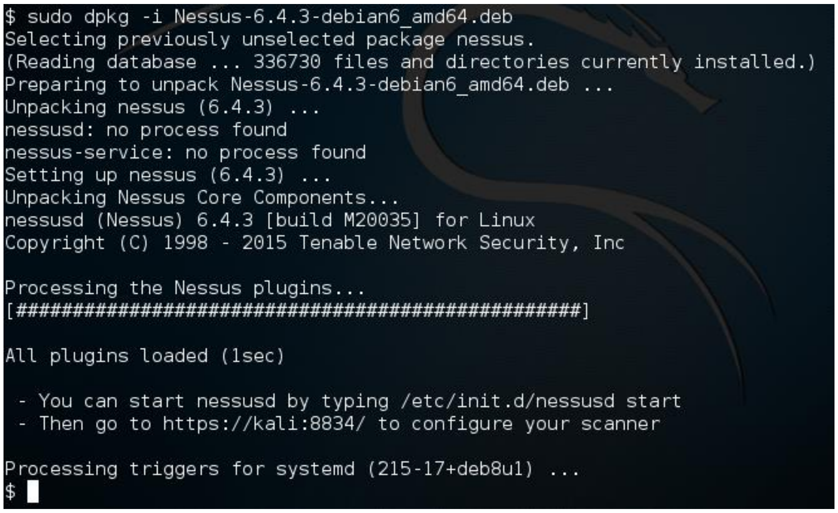
- Change the directory to Downloads. Type **cd Downloads** (remember Linux is case sensitive so be sure to type the capital D)
- Type **ls** again and you should see the file you just downloaded (**Nessus-6.4.3-debian6_amd64.deb**. If you have a 32 bit operating system the file will be **Nessus-6.4.3-debian6_i386.deb**.



```
$ ls
Nessus-6.4.3-debian6_amd64.deb
$ 
```

- Type **sudo dpkg –i Nessus-6.4.3-debian6_amd64.deb** (64 bit) (will be a different file if you have a 32 bit OS. In that case type **sudo dpkg –i Nessus-6.4.3-debian6_i386.deb**

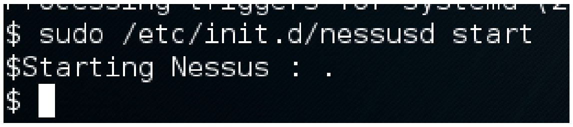
- Enter the password for user1 – **root**
- You should see the following



```
$ sudo dpkg -i Nessus-6.4.3-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 336730 files and directories currently installed.)
Preparing to unpack Nessus-6.4.3-debian6_amd64.deb ...
Unpacking nessus (6.4.3) ...
nessusd: no process found
nessus-service: no process found
Setting up nessus (6.4.3) ...
Unpacking Nessus Core Components...
nessusd (Nessus) 6.4.3 [build M20035] for Linux
Copyright (C) 1998 - 2015 Tenable Network Security, Inc

Processing the Nessus plugins...
[##################################################]

All plugins loaded (1sec)

 - You can start nessusd by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (215-17+deb8u1) ...
$ 
```

Start Nessus

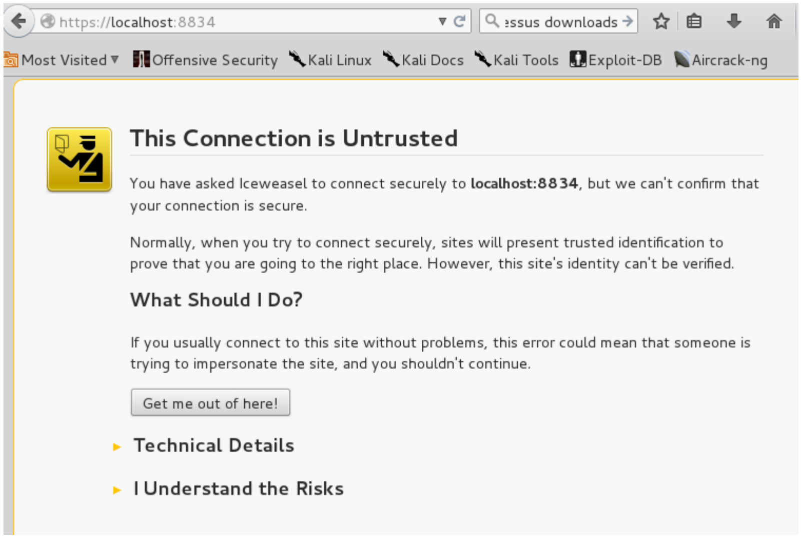
- Follow the directions and start nessusd by typing **sudo /etc/init.d/nessusd start** and hit **enter.** You should see **Starting Nessus: .**



```
$ sudo /etc/init.d/nessusd start
$Starting Nessus : .
$ 
```

Nessus Connection and Configuration

- Now Open **Iceweasel** and enter https://localhost:8834 and hit **enter**
- You should see an error **This Connection is Untrusted**



This Connection is Untrusted

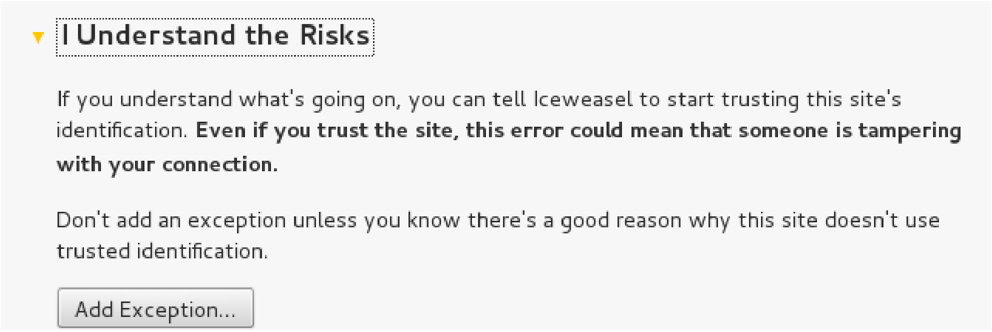
You have asked Iceweasel to connect securely to **localhost:8834**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

- Click **I Understand the Risks**
- Click **Add Exception**

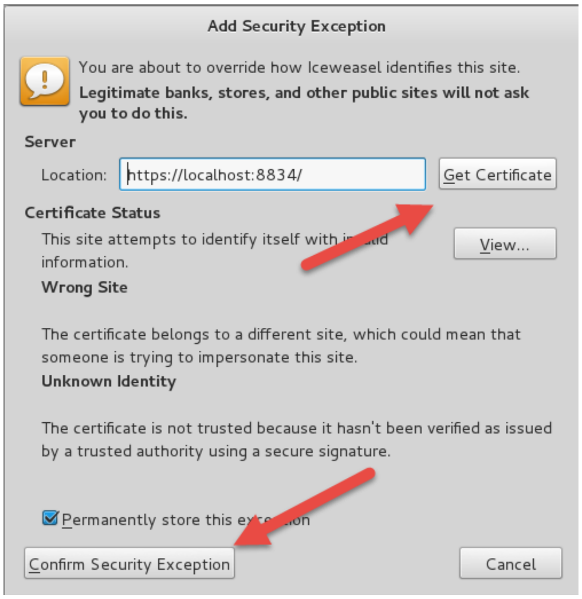


I Understand the Risks

If you understand what's going on, you can tell Iceweasel to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

- Click **Get Certificate** and **Confirm Security Exception**



Add Security Exception

You are about to override how Iceweasel identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://localhost:8834/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

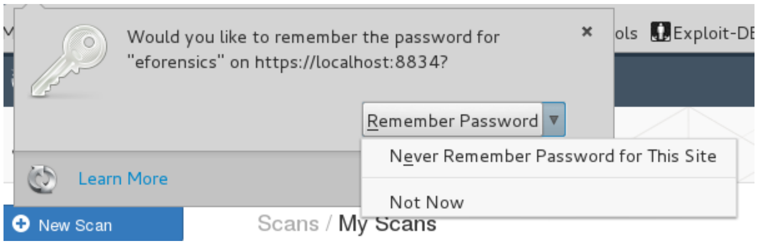
The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

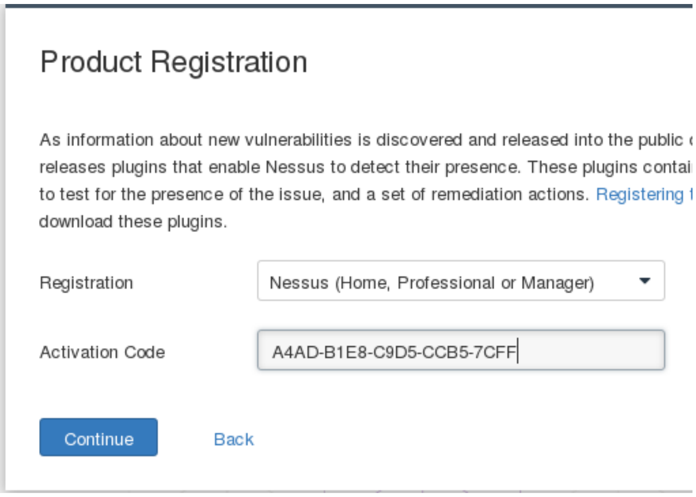
- You will be presented with the Nessus welcome screen, Click **Continue**
- **Initial Account Setup**
    - Username – **user1**
    - Password – **root**
    - Confirm Password – **root**
- If you are asked if you want to save your password select **Never…**



Would you like to remember the password for "eforensics" on https://localhost:8834?

Activation and Plugins Download

- Enter you activation code from your nessus.txt file and Click Continue



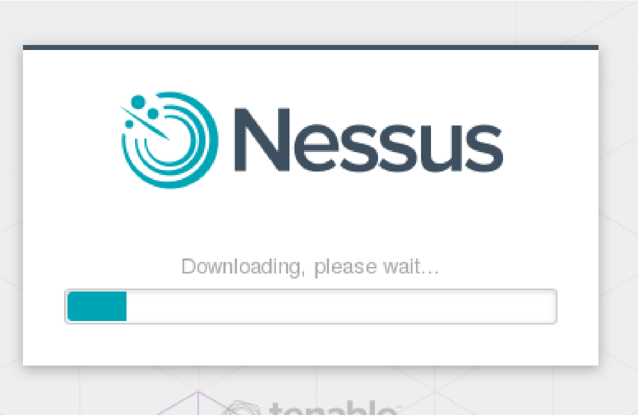
Product Registration

As information about new vulnerabilities is discovered and released into the public
releases plugins that enable Nessus to detect their presence. These plugins contai
to test for the presence of the issue, and a set of remediation actions. Registering
download these plugins.

Registration: Nessus (Home, Professional or Manager)

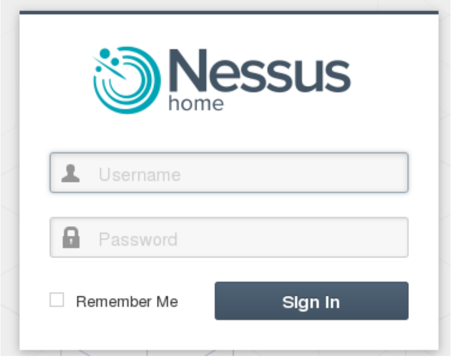
Activation Code: A4AD-B1E8-C9D5-CCB5-7CFF

- Wait for the plugins to download

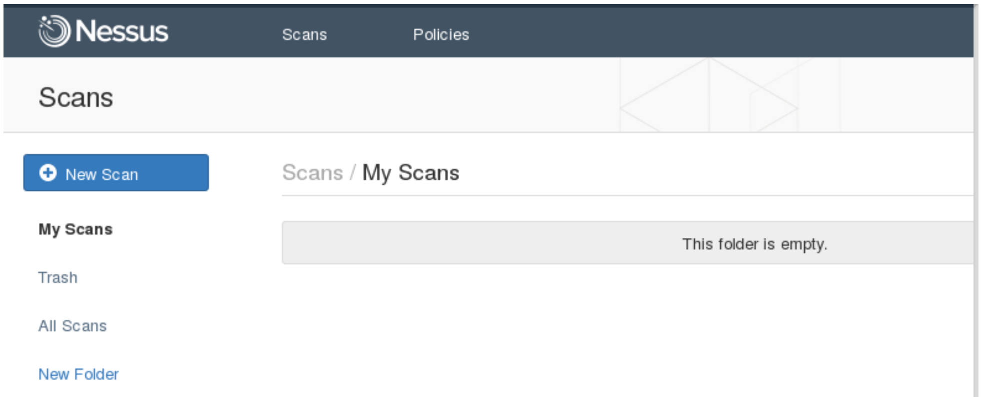


Downloading, please wait...

- When the update is complete you will be at the logon screen
- Enter the username of **user1** and a password of **root** then Click **Sign In**



- You will now be at the Nessus Main Screen



This folder is empty.

- Let’s create a new folder for our scans called **user1.**
- Click on **New Folder,** enter **user1,** and Click on **Create**
- You will now see the user1 folder under My scans
- Now we are ready for scanning

Nessus Scan

- Click on **New Scan**
- Select **Basic Network Scan**
- Enter the following Information
  - Name – **Basic Scan Bee-box**
  - Description Basic Scan bee-box
  - Folder – user1
  - Scanner – Local Scanner
  - Targets enter the ip addresses from Bee-Box that you wrote down earlier.

- Click on **Save** and Nessus will conduct a scan of the most common ports
- Wait for the scan to finish and the green circle will be replaced with a gray checkmark.
- Click on the completed scan and review the results

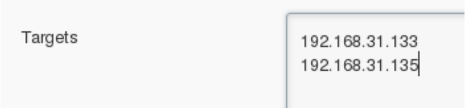
- Click on **New Scan**
- Select **Basic Network Scan**
- Enter the following Information
  - Name – **Basic Scan OWASP**
  - Description Basic Scan OWASP
  - Folder – user1
  - Scanner – Local Scanner
  - Targets enter the ip addresses from OWASP that you wrote down earlier.

- Click on **Save** and Nessus will conduct a scan of the most common ports

- Wait for the scan to finish and the green circle will be replaced with a gray checkmark.
- Click on the completed scan and review the results

Nessus Scan Two Hosts

- Click on **New Scan**
- Select **Basic Network Scan**
- Enter the following Information
    - Name – **Basic Scan 2hosts**
    - Description Basic Scan 2hosts
    - Folder – user1
    - Scanner – Local Scanner
    - Targets enter the ip addresses from OWASP and Bee-Box that you wrote down earlier.

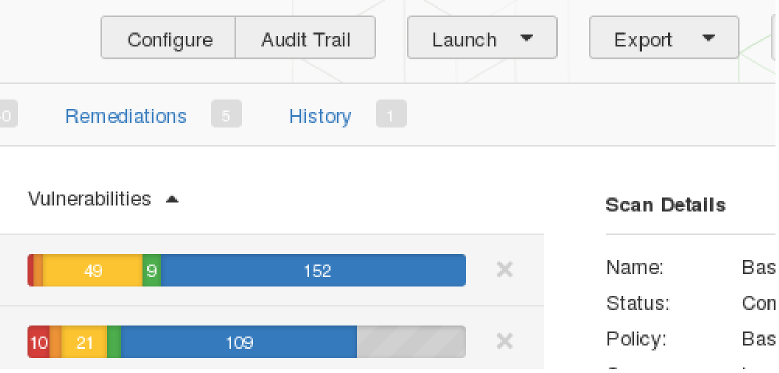


Targets
192.168.31.133
192.168.31.135

- Click on **Save** and Nessus will conduct a scan of the most common ports
- Wait for the scan to finish and the green circle will be replaced with a gray checkmark. This will take a while as it is scanning 2 hosts.
- Click on the completed scan and review the results

Report Executive Summary

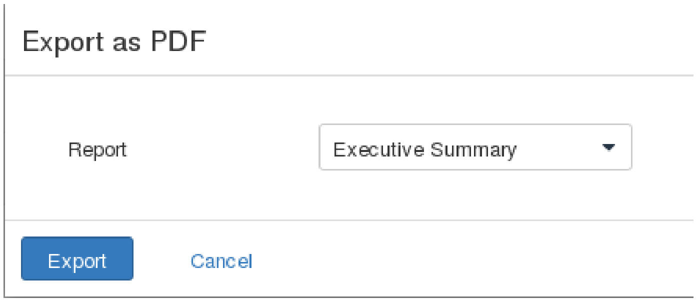
- Click on **Export**



Scan Details

Name: Bas
Status: Con
Policy: Bas

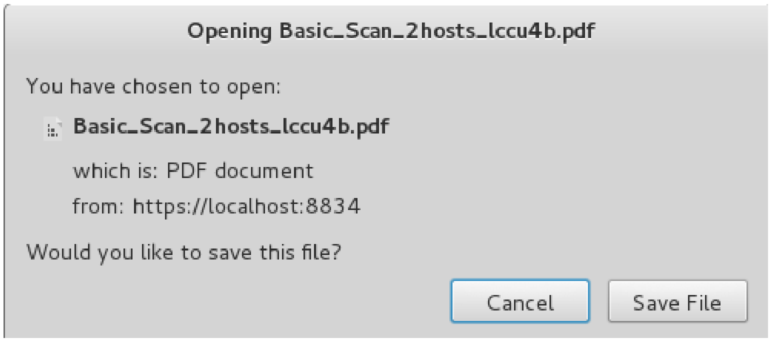
- Select **PDF**
- Accept **Executive Summary** and Click on **Export**



Export as PDF

Report: Executive Summary

- You will now be asked if you want to save the file. Click **Save File**



Opening Basic_Scan_2hosts_lccu4b.pdf

You have chosen to open:

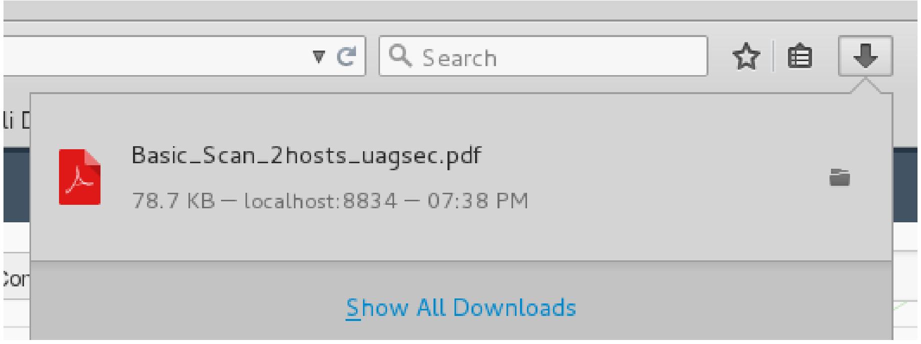
Basic_Scan_2hosts_lccu4b.pdf

which is: PDF document

from: https://localhost:8834

Would you like to save this file?

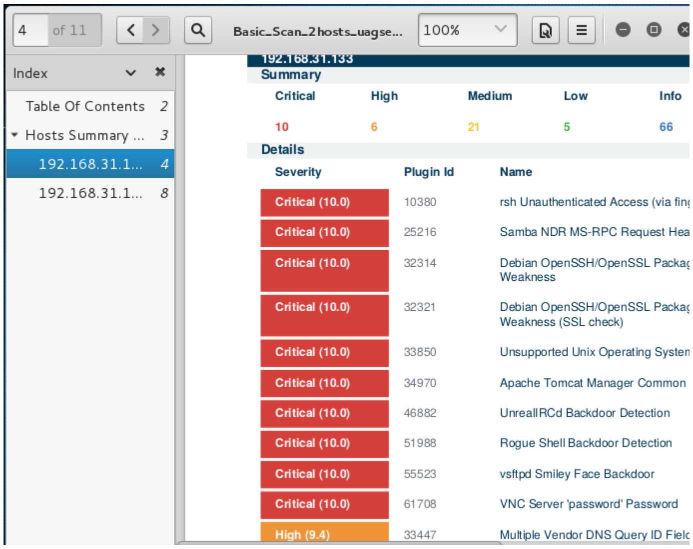
- Now click on the down arrow and you will see the pdf file. Click on the pdf file to open it



Basic_Scan_2hosts_uagsec.pdf

78.7 KB — localhost:8834 — 07:38 PM

- The Nessus Report will now display on your screen
- The executive summary provides the vulnerability information for each host in order of severity.
- Change the view to be 100% and then click on the first ip address



192.168.31.133

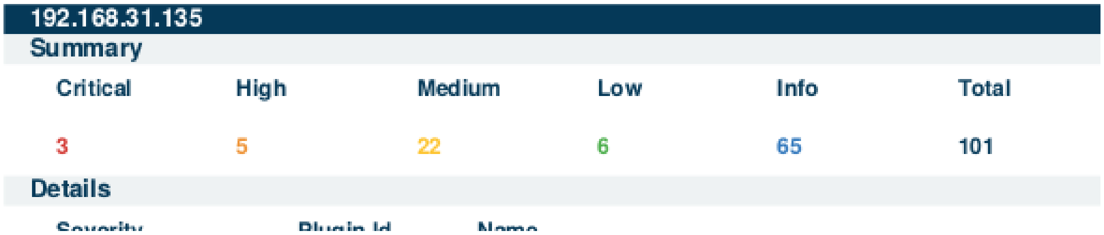
Summary

Critical	High	Medium	Low	Info
10	6	21	5	66

Details

Severity	Plugin Id	Name
Critical (10.0)	10380	rsh Unauthenticated Access (via fin
Critical (10.0)	25216	Samba NDR MS-RPC Request Hea
Critical (10.0)	32314	Debian OpenSSH/OpenSSL Packa Weakness
Critical (10.0)	32321	Debian OpenSSH/OpenSSL Packa Weakness (SSL check)
Critical (10.0)	33850	Unsupported Unix Operating Systen
Critical (10.0)	34970	Apache Tomcat Manager Common
Critical (10.0)	46882	UnrealIRCd Backdoor Detection
Critical (10.0)	51988	Rogue Shell Backdoor Detection
Critical (10.0)	55523	vsftpd Smiley Face Backdoor
Critical (10.0)	61708	VNC Server 'password' Password
High (9.4)	33447	Multiple Vendor DNS Query ID Fielc

- At the top of the screen you will notice the summary of each severity by number



192.168.31.135

Summary

Critical	High	Medium	Low	Info	Total
3	5	22	6	65	101

Details

Severity Plugin Id Name

- Go through the report and look at all the detail it provides. This is an executive summary you can provide to show vulnerabilities by severity so that the client knows what issues they need to address in order of importance.
- Select the **next IP address** and look at the detail for that host
- When you are done looking at the report **Close it**

Thanks for your attention I hope this course has helped you on your way to become an ethical hacker…