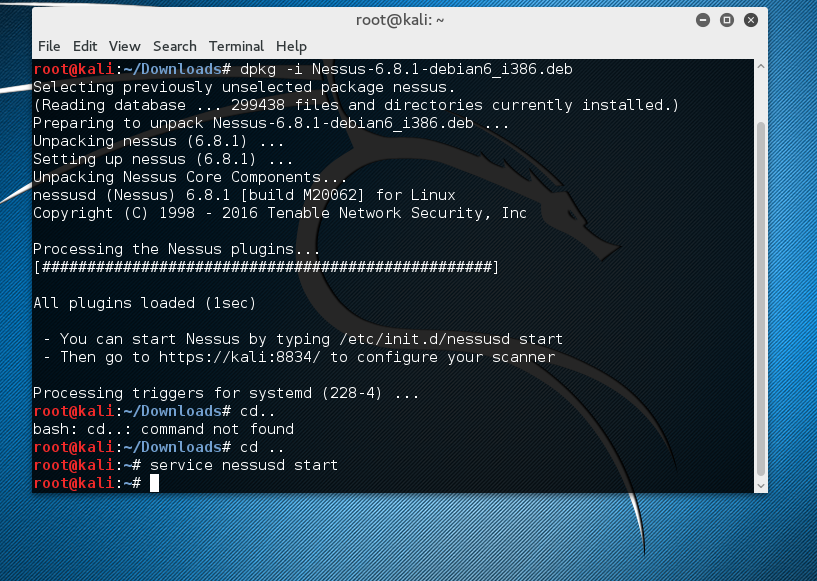
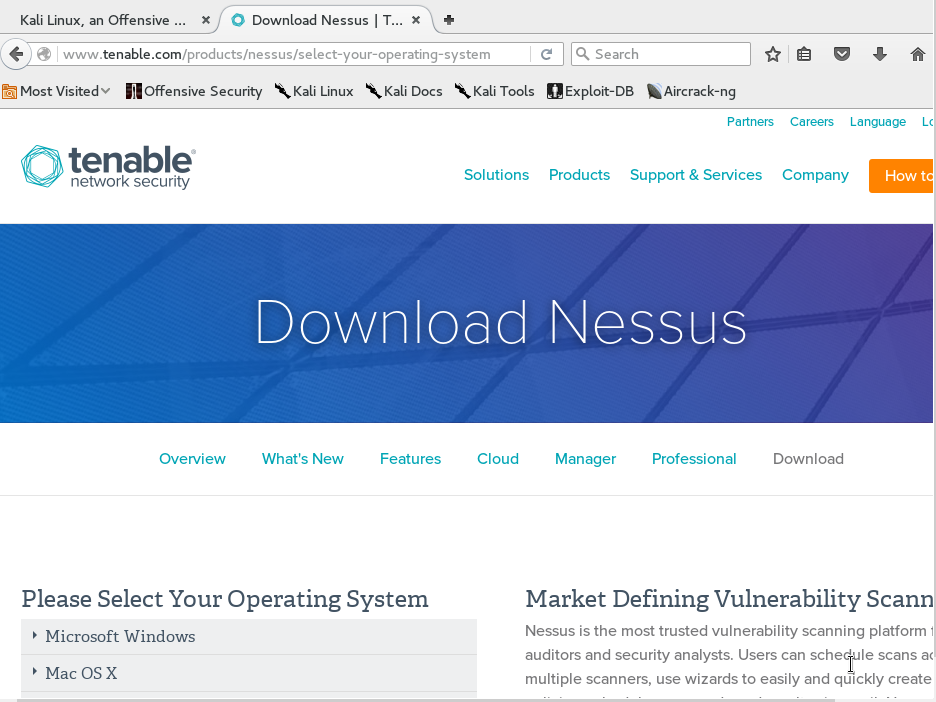
**Provide a short step by step instruction on setting up Nessus.**

Nessus:

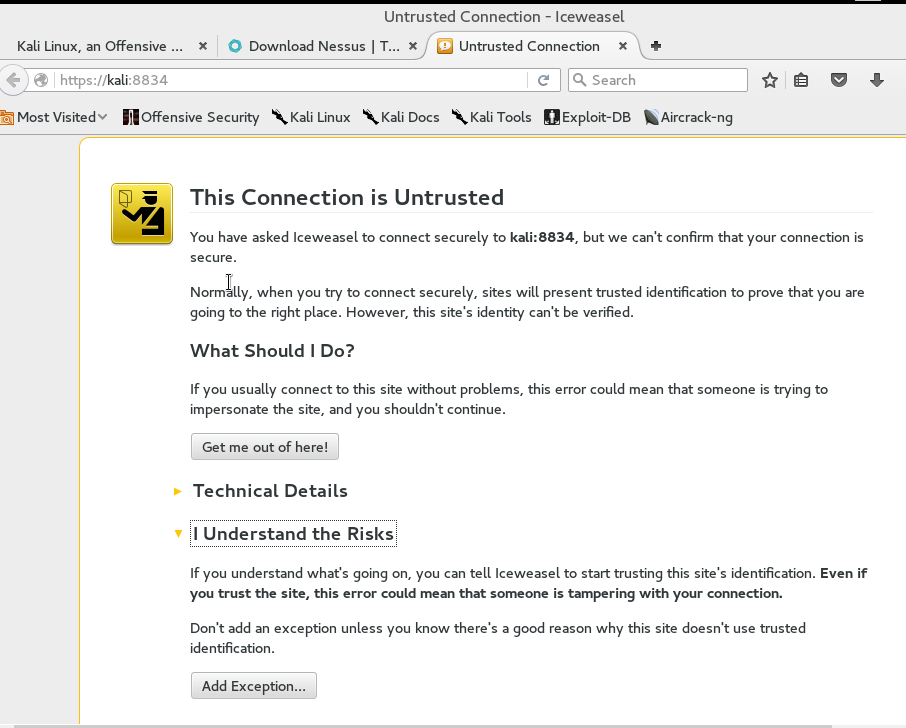
As I have said in the previous discussion Nessus is a vulnerability scanner. I decided to download and install Nessus on a Kali Virtual Machine. I then gave it a test on my own network at home. I actually found some vulnerabilities that I need to take care of.

First:You may need to go to Nessus.com and download the appropriate client. Unpacking Nessus 6.8.1 in linux and Starting the nessusd service. We also got the Kali url for the web ui for the nessus scanner.

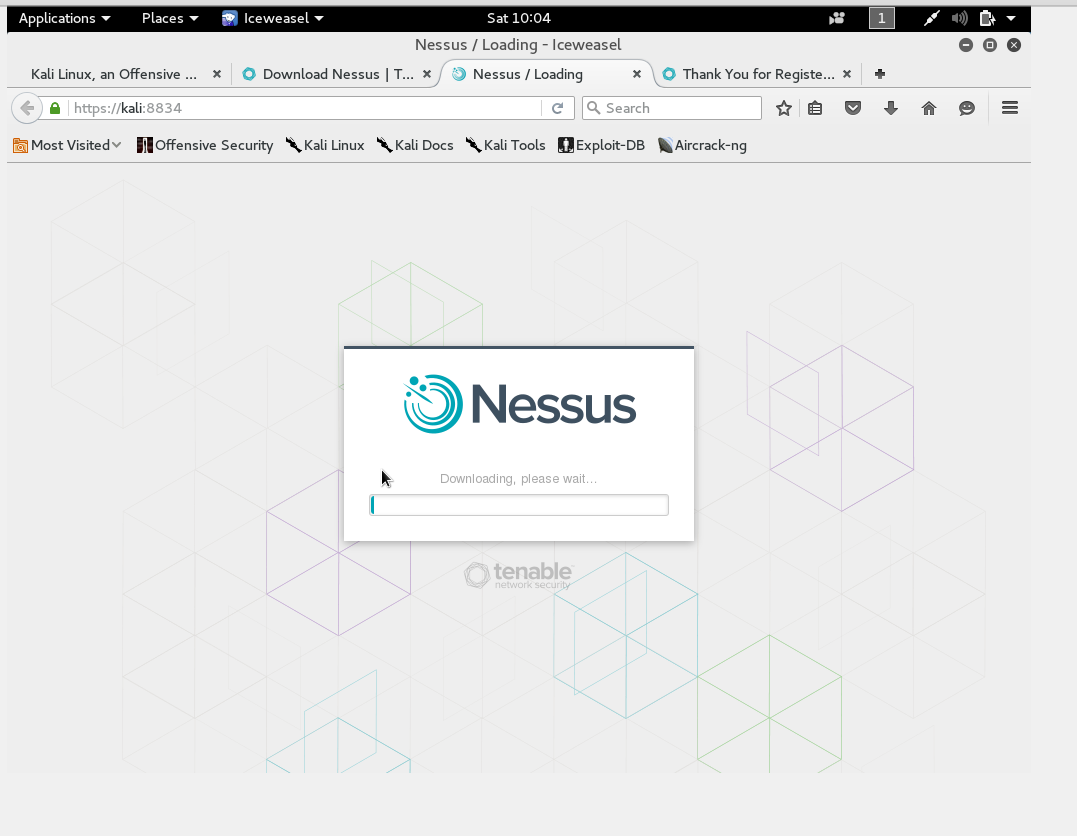




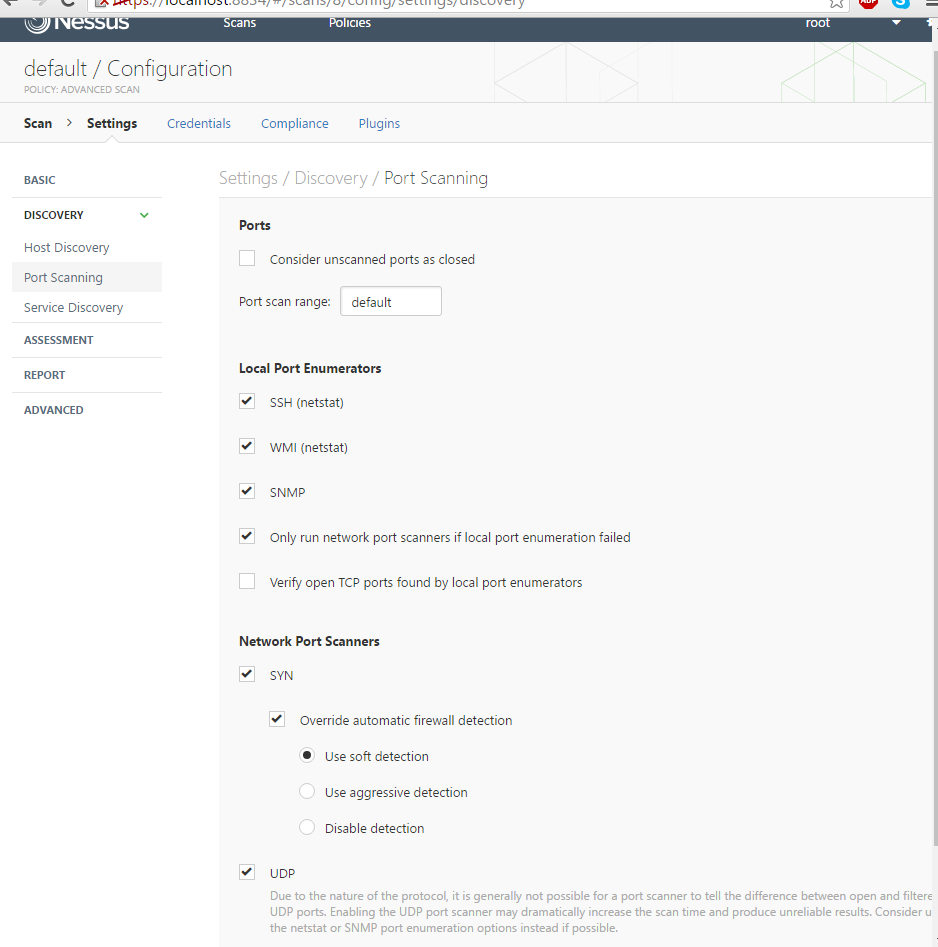
Second: Navigating to <https://kali:8834> URL. Also confirming Security exception for the website.



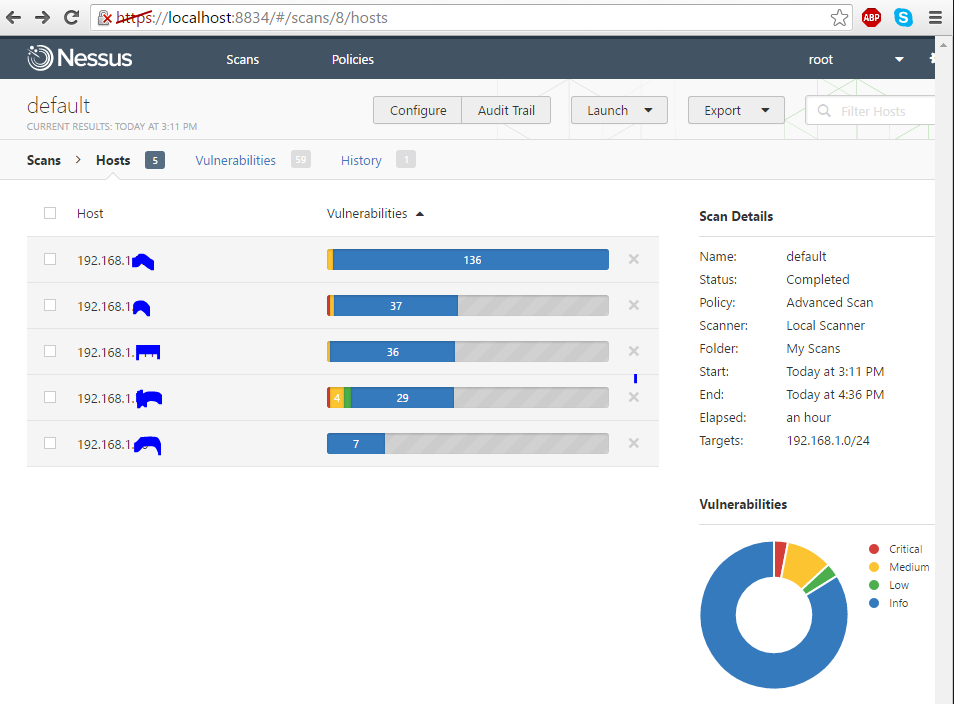
Third:. It will then bring you to a user and password registration page. You will have to input your activation key and activate your nessus. If you haven't gone to the website and retrieved your activation key you will need to register. Wait for Nessus to download and initialize.



Fourth: You will then be brought to the Nessus UI page. To start a scan you will need to customize your first scan in order to scan for vulnerabilities. Nessus has a whole range of different vulnerabilities checks.



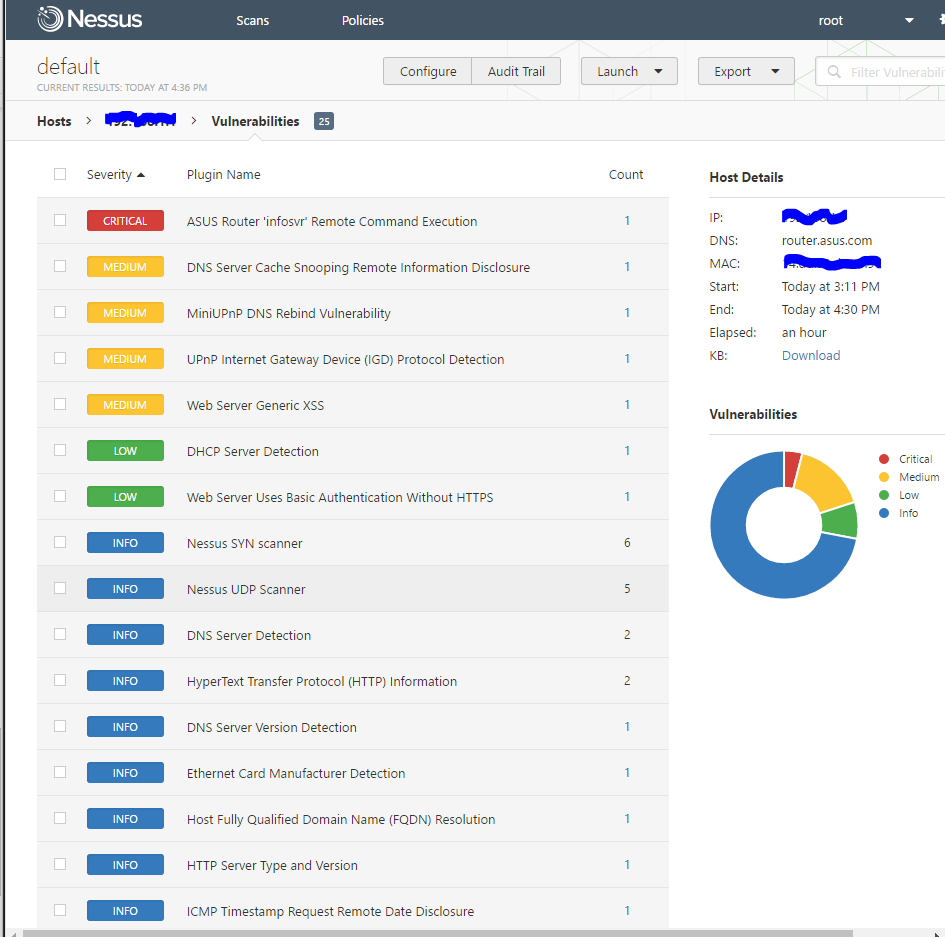
Fifth: My scan of my network.



<https://www.youtube.com/watch?v=h6QYg5h35Tc>

**After reviewing the above, where can potential threats and vulnerabilities originate?**

Looking at my router after the Nessus scan you can see a lot of different vulnerabilities. ASUS Router ‘infosvr’ remote command execution vulnerability for one. “The remote device is an ASUS router that contains firmware which is affected by a flaw in its 'infosvr' service due to not properly checking the MAC address of a request. An unauthenticated, remote attacker, using a crafted request to UDP port 9999, can exploit this to run arbitrary commands or access configuration details (including passwords) on the device.” - Nessus Knowlege Base. Nessus is so nice this way, it tells you what the vulnerability is and then tells you the best ways to secure the vulnerability. They also give you other resources to look up to better secure my device. Looks like I just have to upgrade my routers firmware. Which I did.



We did an vulnerability assignment for CSIA 6200. Where we uses different vulnerability tools. Some of these tools are NetDiscover, Nmap, and Nbtscan. NetDiscover is a tool on kali or backtrack linux that allows an user to discover different networks, and nodes on the networks. Nmap is is another security vulnerability scanner, majority of what it is used for is port scanning. Nbtscan is a an IP scanning tool for scanning NetBIOS information.

The book describes how we use a secure network design to ensure that we have our networks segmented properly. The best way to help do this is to make sure we are monitoring and controlling traffic on our network. Best security practice is implementing firewalls, and Intrusion detection systems both inside and outside of our network, also using VPN to secure our connections from the outside in. In the undergraduate network security class we had a project where we set up an honeypot. A honeypot is a decoy history that traps hackers, or tracking/logging how the hacker broke into the honeypot. Honeypots are designed to lure hackers to try to attack the honeypot. If multiple honeypots are set up on one network it is called a honeynet. Potential vulnerabilities can originate from anywhere. As I stated before in a previous post I stated, “These vulnerabilities come in different categories, physical protections, and Cyber Security. We have to have access for vulnerabilities in both the physical and cyber individually, also together. Understanding the entire system and the security behind that system allows security professionals to account for all vulnerabilities in a system. There are two methods of attack can originate from two directions, from the inside and outside. An example of an inside attack is employee with access tries installs a Malware on a POS machine skimming credit card information. An example of an attack from the outside is seal team six breaking into bin laden compound to kill bin laden.”

<https://nmap.org/>

<http://unixwiz.net/tools/nbtscan.html>

<http://www.backtrack-linux.org/forums/showthread.php?t=8154>

<https://www.techopedia.com/definition/10278/honeypot>

<http://proquest.safaribooksonline.com.proxy.li.suu.edu:2048/book/networking/security/9780128007440/the-basics-of-information-security/title_page_xhtml_2?query=((The+Basics+of+Information+Security%2c+2nd+Edition))#X2ludGVybmFsX0h0bWxWaWV3P3htbGlkPTk3ODAxMjgwMDc0NDAlMkZzdDAwMjVfY2hwMDEwX3hodG1sJnF1ZXJ5PSgoVGhlJTIwQmFzaWNzJTIwb2YlMjBJbmZvcm1hdGlvbiUyMFNlY3VyaXR5JTJDJTIwMm5kJTIwRWRpdGlvbikp>

<http://hackercool.com/2013/08/how-to-install-nessus-in-kali-linux/>

<http://www.geekyshows.com/2013/07/how-to-use-netdiscover-in-kali-linux.html>

<http://hackercool.com/2016/02/how-to-setup-openvas-in-kali-linux/>