**Provide a short comparison between Nessus and OpenVAS.**

Nessus: Is a remote security vulnerability scanning tool. We used Nessus in an assignment last semester. It was an very useful tool in finding Vulnerabilities in systems, using a web interface. Nessus has a variety of different customisable scans. The great thing about Nessus is the ability to scan client software too. These vulnerability scans are compared to known standards, but you also have the ability to customize your own. These scans include malware and botnets which we did in our last class. Something new I learned about Nessus is the Patch management integration, nessus has the ability to check if your patches are uptodate with any errors. Also Nessus will patch and reinstall damaged patches. I think something else new about Nessus is the Mobile device audits, where it is testing whether a phone is vulnerable or not. When I used Nessus I found that if was very easy to setup, and very detailed in its vulnerability scans, plus it is free for home use. :)

<https://www.youtube.com/watch?v=r_pDVhNoYr0>

<https://www.youtube.com/watch?v=sqFXXvaA8p4>

<http://resources.infosecinstitute.com/network-scanning-using-nessus/>

Here are some Scans I did in the last class in Nessus:

****

OpenVas: Last Semester we also did a vulnerability scan using OpenVAS. What I can remember was not understanding how to work it very well. I can remember it being taking a very long time to do a complete can, but that is understandable. OpenVAS is also an Vulnerability scanner, with a web interface. The great thing about OpenVAS is it is an open source software, that has integrated nmap(port scanner) into it’s scans. In combination with other programs like Nessus you will find the majority of your vulnerabilities.

<https://www.youtube.com/watch?v=PTkOfEz8eMM>

<https://hackertarget.com/nessus-openvas-nexpose-vs-metasploitable/>

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

As Anish from last week's discussion said, we as security professionals need to look at how we secure something not just on the surface level but a complete overview of vulnerabilities. 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.

The video below was given to us by Professor Robertson last semester but it applies very well here:

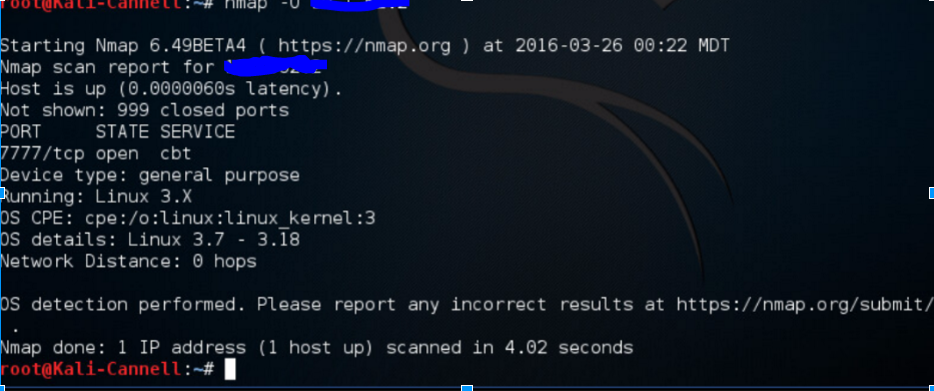
<https://www.youtube.com/watch?v=Hh5NEpJZGZw>

<https://msdn.microsoft.com/en-us/library/cc723507.aspx>

**What security technologies beyond Nessus and OpenVAS are available to help secure networks.**

Nmap: is another security vulnerability scanner, majority of what it is used for is port scanning. Port scanning is when an application is used to probe a host to determine if the host has any open ports. Open ports are bad because it is a vulnerability that can allow exploits into a hosts machine from a malicious user. Nmap can be used as a Network security tool to determine if their are any ports that are open which might violate security policies, and help secure a system. Nmap is ran on linux and comes prepackaged in Kali and backtrack. I have used Nmap alot in past classes and at work it is a very valuable tool.

<https://nmap.org/>



Metasploit: is another Security Vulnerability scanning tool. I personally havent used Metasploit yet, but talking with one of the security guys at my work he highly recommends learning this if you are going to do any penetration testing. Penetration testing is another way of saying vulnerability scanning, except the whole purpose is to view it from the perspective of the hacker. Metasploit is also an open source program, designed to use exploits against remote targets.

<https://help.rapid7.com/metasploit/index.html>

<https://www.youtube.com/watch?v=TCPyoWHy4eA>

Aircrack-ng: Also an Security Vulnerability scanning tool. This is used specifically as the name hits towards Wireless networks. Aircrack is a packet sniffer, like wireshark but unlike wireshark which is an analytic tool aircrack is used as a WEP/WPA2 Cracking and analysis. Just like Nmap this is also an linux tool, and comes prepackaged in kali and backtrack linux OS’s and of course is opensource. This can be used in WarDriving, which is when an attacker drives around searching for vulnerable wireless networks in the hope of access to someone's private network. Aircrack sniffs out traffic on 802.11a,b,and g traffic and is a virsital tool, when used in combination with some other tools like airdecap-ng which decrypts wep and wpa encrypted files, or airdump-ng.

<https://www.youtube.com/watch?v=GLO9HGDwOY0>

<https://www.aircrack-ng.org/doku.php?id=getting_started>

<https://books.google.com/books?id=WHcjc42p_MQC&pg=PA227&lpg=PA227&dq=aircrack+practical+uses&source=bl&ots=59xQs1nmwX&sig=tuXcWENsb-41RzMnDcCggLeIZnI&hl=en&sa=X&ved=0ahUKEwiiy4S29vHOAhWI4SYKHTEYBSIQ6AEIRDAI#v=onepage&q=aircrack%20practical%20uses&f=false>