1. What is the process of vulnerability analysis?

Vulnerability analysis consists of several steps:

* Defining and classifying network or system resources
* Assigning relative levels of importance to the resources
* Identifying potential threats to each resource
* Developing a strategy to deal with the most serious potential problems first
* Defining and implementing ways to minimize the consequences if an attack occurs.

If security holes are found as a result of vulnerability analysis, a vulnerability disclosure may be required. The person or organization that discovers the vulnerability, or a responsible industry body such as the Computer Emergency Readiness Team ([CERT](http://whatis.techtarget.com/definition/CERT-Computer-Emergency-Readiness-Team)), may make the disclosure. If the vulnerability is not classified as a high level threat, the vendor may be given a certain amount of time to fix the problem before the vulnerability is disclosed publicly. The third stage of vulnerability analysis (identifying potential threats) is sometimes performed by a [white hat](http://searchsecurity.techtarget.com/definition/white-hat) using [ethical hacking](http://searchsecurity.techtarget.com/definition/ethical-hacker) techniques. Using this method to assess vulnerabilities, security experts deliberately probe a network or system to discover its weaknesses. This process provides guidelines for the development of countermeasures to prevent a genuine attack.

1. What are some common network security vulnerabilities and how attackers take advantage of it?

The top 5 network security vulnerabilities are:

Missing patches

All it takes for an attacker, or a rogue insider, is a missing patch on a server that permits an unauthenticated command prompt or other backdoor path into the web environment. Sure, we have to be careful when applying patches to servers but to not apply patches at all (I often seen missing patches dating back 10+ years) just makes it too easy.

Passwords shouldn’t even be part of a network security vulnerability discussion knowing what we now know. However, many web applications, content management systems, and even database servers are still configured with weak or default passwords. Who needs file inclusion or SQL injection when the file system or database can be accessed directly?

One of the biggest, most dangerous, assumptions is that everything is well in the firewall because it’s been working fine. Digging into a firewall rulebase that has never been analyzed will inevitably turn up serious configuration weaknesses that allow for unauthorized access into the web environment. Sometimes it’s direct access while other times it’s indirect from other network segments including Wi-Fi – parts of the network that may have been long forgotten.

### Mobile devices

Phones, tablets, and unencrypted laptops pose some of the greatest risks to web security. Think about all the VPN connections, cached passwords in web browsers, and emails containing sensitive login information that you – and likely everyone else responsible for managing your web environment – have stored on mobile devices. The use of unsecured (and rogue) Wi-Fi via mobile devices is the proverbial icing on the cake.

### USB Flash Drives

The dangers of these innocent-looking portable devices have been known for long enough. But still, all that Edward Snowden reportedly needed to walk away from the National Security Agency building with a cache of national secrets was a USB flash drive. USB drives are also one of the most common ways a network can get infected from inside a firewall.

3.What does the report of [Nessus](http://mydy.dypatil.edu/rait/mod/quiz/view.php?id=102218) tell us? How we can get benefit of it.

 Nessus reports can display vulnerabilities in different ways:

* **Suggested Remediations** — Nessus summarizes the actions to take that address the largest quantity of vulnerabilities on the network. For example, Nessus will recommend that “Taking the following actions across 2 hosts would resolve 42% of the vulnerabilities on the network” and proceed to list the details of those specific vulnerabilities.
* **Vulnerabilities Grouped by Plugin** — Lists each vulnerability found during your scan and the affected hosts. Systems administrators will find it easy to read this report and fix the problems that have been identified.
* **Vulnerabilities Grouped by Host** — Lists each host found during the scan and its associated vulnerabilities. Systems administrators will often use this report to address specific issues with certain hosts, follow-up scans, PCI scans, and targeted assessments.