**Summary Report**

Vulnerability scanning involves inspecting any weak points and security loopholes in a computer or network that can be used to exploit the system. During vulnerability scanning, scanners detect and classify weaknesses in computers and networks and also predict effectiveness that could be done by any countermeasures taken. Vulnerability scans can, however, pose risks to the machines being targeted for scans. Scans can thus cause issues like reboots, errors, and a reduction of productivity.

According to the research conducted by the stated group on Amazon Web Services, which aimed to gather information and reconnaissance, I agree with the findings they came up with. The three tools used, Nmap, Whois, and Nikto, are commonly used in performing scans and penetration testing.

The Nmap tool is used for port scanning. The ports are tested to determine their state. There are six port states which Nmap recognizes, namely open, closed, filtered, unfiltered, open|filtered, and closed|filtered. (Pinkard & Orebaugh,2011). An open state indicates that an application is active, which means accepting TCP connected or UDP ports. Finding an open port is usually the main goal during port scanning. Normally open ports are usually an avenue for security attacks. Attackers normally want to exploit open ports while system administrators aim at closing and protecting them with firewalls.

Closed port state indicates that the port is accessible; it receives and responds to Nmap packets; however, there is no application listening to it. Finally, the filtered port state is returned when Nmap cannot determine if the port is open or closed because filtering packets prevents Nmap probes from reaching the port. These ports are always a frustration to attackers because they give so little information to them.

Unfiltered port state means that the port being scanned is accessible, but Nmap cannot determine whether it's closed or open. Open|filtered state ports are classified so if Nmap is unable to determine whether the port lies under the open or filtered category. This occurs when open ports give no response. Closed|filtered state is used when Nmap cannot determine if the port is closed or filtered.

Nikto is a lightweight web server scanner used to perform tests on web servers for multiple items, including potentially harmful programs or files. It checks for outdated versions of over 1250 servers and outlines specific version problems. It also identifies server misconfigurations, including the presence of multiple index files and HTTP options of the server. Finally, it also checks for default files and programs. Nikto is updated regularly; hence it provides reliable results on any latest vulnerabilities.

Whois is widely used on the internet to identify the owner of a domain and get into contact with them. Records from whois have been valuable resources to maintain the integrity of any domain name during the registration and website ownership process. The whois record contains contact information associated with the owners of the domain name. However, whois record information is provided during domain name registration. Over time domain name details change; thus, the owners are required to update their records to improve whois accuracy. (Liang & Yang,2010)

**REFERENCES**

Liang,P.,Yang,J.,( 2010 )Analysis on cloud-based security vulnerability assessment- ieeexplore.ieee.org

Pinkard,B.,Orebaugh, A.,(2011)Your guide to network scanning-books.google.com