Vulnerability Scanning System for attached devices on a network

Abstract:

Vulnerability scanning in a network is considered the main part during the security process implementation. The aim of this project is to design and implement an application that responsible for running vulnerability scanning including host scan, ping, port scan, and etc. in any network that your pc is connected to it and running this application. Separate tools are available in order to do the vulnerability scanning which make the performance of the pc low, along with the cost of buying them if compared with using this application. It identifies and creates a list of devices that are connected to the network depends on a specific range of IPs.

For each device, “ping” command is sent to check the reachability, it also attempts to identify the IP address of a device if a url is available, along with other information such as used operating system, user accounts and etc. After building up the list of devices, the vulnerability scanner checks the ports that are open in two cases: all ports and specific range of ports. The result is a list of all the devices found and identified on the network, highlighting any ports that are open. It also can scan any web application url to look for IP, domain name, header information and etc.