**Network Security - Port Scanner**

**Nmap port scanner**

Nmap ("Network Mapper") [ http://www.insecure.org/nmap/Links to an external site.Links to an external site. ] is an open-source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap is free software, available with full source code under the terms of the GNU GPL. Nmap is available for Windows and Linux.

The user manual provides an extensive command list for all kind of functions nmap could provide; explore it to learn more features.

Here is also tons of online video teaching you how to use nmap, just type in the keyword “nmap” in Youtube and you will get them.

Assignment:

After installing Nmap,

Launch “Command Prompt” by typing “cmd” in “start> run”

Enter into C:\program files\nmap\, which should be the default directory for your installation

Enter command “nmap -P0 -O -A ”+ an IP address or a domain name, and wait for a few minutes to see the results; Here “–P0” means scan all ports; “-O” help you identify the OS running on the host computer; “-A” enable OS detection, version detection, script scanning, and traceroute. Make sure there is a space between the command and the option as well as between options!

Use the same command above to scan a computer in your house and see the results – you may use domain name or IP address of the computer. For example, “nmap –P0 -O -A 192.168.0.1”

If you can obtain agreement from a remote host owner, you may scan the host/server with its domain name or IP address.

Please answer the following questions in your lab report

1) Submit answers to the following questions based on the reports you generated.

a) Did you find any vulnerabilitywith the computer you scanned?

b )What operating systems are running on the hosts you visited?

c) List several services running on each computer?

d) Identify one high severity vulnerability for each computer (if there is one). Describe the vulnerability and discuss control(s) to minimize the risk from the vulnerability.

Choose a submission type