Hack to Learn – Port Scanning

1. What is computer hacking?
2. What is a server port?
3. Why is it important to know which ports are open, and which server programs are listening on the open ports?
4. Why should you only scan ports of the servers you are responsible for?

Ports are like little doors on your system. Most packets leaving your machine come out of a certain door. They are destined for another door on another system. There are two different protocols that use ports: TCP and UDP. Each of these two protocols has 65,536 different ports. Various Internet services listen on certain well-known doors. For example, Web servers usually listen on TCP port 80. Mail servers usually listen on TCP door port 25.

Security breach scenario: An attacker launches a port scan to see what ports are open, with a listening service, on your machine. A port scan attack, therefore, occurs when an attacker sends packets to your machine, varying the destination port. The attacker can use this to find out what services you are running and to get a pretty good idea of the operating system and programs you have. System Administrators should harden the firewall and minimize the services allowed through it in order to prevent harmful attacks.

List of ports and associated vulnerabilities: http://www.speedguide.net/ports_sg.php

To find which ports your computer has open, run the following command:

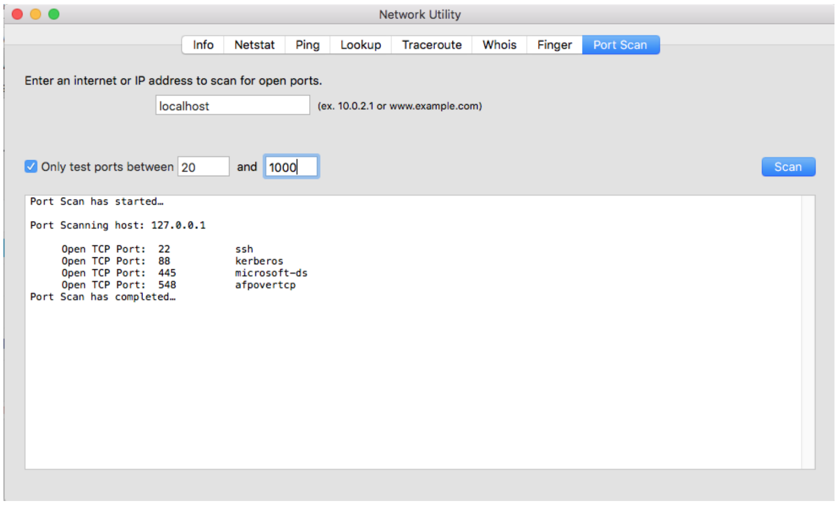
Windows

```
netstat -ano|find /i “listening”
```

or

```
netstat -ano|find /i “established”
```

Macintosh



Enter an internet or IP address to scan for open ports.

localhost (ex. 10.0.2.1 or www.example.com)

☑ Only test ports between 20 and 1000

```
Port Scan has started…

Port Scanning host: 127.0.0.1

     Open TCP Port:  22          ssh
     Open TCP Port:  88          kerberos
     Open TCP Port:  445         microsoft-ds
     Open TCP Port:  548         afpovertcp
Port Scan has completed…
```

Python Port Scanner

```
import socket
import subprocess
import sys
from datetime import datetime
subprocess.call('clear', shell=True)
remoteServer    = input("Enter a remote host to scan:")
remoteServerIP  = socket.gethostbyname(remoteServer)
print ("-" * 60)
print ("Please wait, scanning remote host", remoteServerIP)
print ("-" * 60)
try:
    for port in range(20,100):
        print('Connecting on port ', port)
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.settimeout(5)
        result = sock.connect_ex((remoteServerIP, port))
        if result == 0:
            print ("Port {}: \t Open".format(port))
        sock.close()
except KeyboardInterrupt:
    print ("Thank you for using the port scanner!")
    sys.exit()
except socket.gaierror:
    print ('Hostname could not be resolved. Exiting')
    sys.exit()
except socket.error:
    print ("Couldn't connect to server")
    sys.exit()
print ('Scanning Completed')
```

Homework

1. Enhance the port scanner such that it displays open ports only.
2. Enhance the port scanner by displaying how long it took the program to scan all the ports. Hint: use datetime.now()