Intro to Cybersecurity

Network Ports

Ports

The IP address is used to communicate from one host to another (one computer to another).

The port is used to communicate from one process running in one host to another process running in another host.

Ports

The human analogy would be sending a package via post mail service. IP addresses are like the address to a home, and the port is the person that lives in the home to which the package is directed.

Port

Ports are a 16 bit positive number.

2^{16} = 65536 numbers, 0 - 65636

Clients need to know, not only the IP address, but also the port number of a server process.

Server Port

Common application services have particular assigned port numbers.

Some common application services are:

- http, listen port 80
- https, 443
- ssh, 22
- smtp, 25
- dns, 53

Services and assigned ports can be found at /etc/services or http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Client Port

Client port number is assigned randomly in the client operating system.

The client is the one that initiates communications with the server, the server receives the client port address and thus know what port to communicate.

Server unconventional port

When a server use a port different to the conventional port, the user has to specify the client application the server port.

For instance if a web server is running in port 8080 instead of the conventional port 80. The user can specify the port using the : symbol after the server name followed by the port.

http://servername.com:8080

netstat - to list the ports in use

$ sudo netstat -alnp | head

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:875	0.0.0.0:*	LISTEN	12263/rpc.rquotad
tcp	0	0	0.0.0.0:35244	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:719	0.0.0.0:*	LISTEN	962/ypserv
tcp	0	0	0.0.0.0:111	0.0.0.0:*	LISTEN	912/rpcbind
tcp	0	0	0.0.0.0:53810	0.0.0.0:*	LISTEN	12268/rpc.mountd
tcp	0	0	0.0.0.0:43764	0.0.0.0:*	LISTEN	12268/rpc.mountd
tcp	0	0	0.0.0.0:725	0.0.0.0:*	LISTEN	4784/ypbind
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	16300/sshd

In windows:
netstat -bro

Listening port

Knowing what ports are listening in my computer allows me to understand my computer risk for intrusion.

Transport Layer: TCP and UDP

Two basic transport layers (TCP and UDP)

TCP: Transport Control Protocol

TCP establishes a reliable connection where all the packets sent through that connection arrive to the destination in order.

TCP provides reliable transmission, error detection, flow control, and congestion control.

The connection is established via what is called the TCP handshake that involves acknowledges messages.

UDP: User Datagram Protocol

UDP is a connectionless protocol, packets can get lost, and packets can arrive out of order.

UDP does not provide any congestion or flow control. It is a lightweight protocol compared to TCP because of the fewer features.

It is used in protocols that allow few packet loss such as VoIP and video streaming.

Internet apps transport protocols

application	application layer protocol	underlying transport protocol
e-mail	SMTP [RFC 2821]	TCP
remote terminal access	Telnet [RFC 854]	TCP
Web	HTTP [RFC 2616]	TCP
file transfer	FTP [RFC 959]	TCP
streaming multimedia	HTTP (e.g., YouTube), RTP [RFC 1889]	TCP or UDP
Internet telephony	SIP, RTP, proprietary (e.g., Skype)	TCP or UDP

nc - (netcat)

Is a computer networking service for reading from and writing to network connections using TCP or UDP.

nc - (netcat)

In the "client" mode of netcat, you give it an IP Address and a port number, and whatever you type into after pressing enter gets sent to the given address and port using TCP over IPv4.

nc - (netcat)

In the "server" mode of netcat. you give the -l option (listen) and nc then acts like a server, "listening" for a connection request, accepting the first one it receives, then echoing whatever gets sent to it to the screen, and taking whatever gets typed on the screen and sending it to the client whose connection request it accepted.

nc - example

Client Example:

```
$ nc 136.145.181.40 4088
```

Connects to server 136.145.181.40 in port 4088

Server Example:

```
$ nc -l 4088
```

Listen for connections in port 4088

Server must have the IP 136.145.181.40 to work.

nc - (netcat)

Netcat with the -u option (UDP) uses UDP instead of TCP. Since this is connectionless, the server version accepts datagrams from any and all who send them, rather than making a connection with one client. As another consequence, the UDP server doesn't exit just because one of the clients exits.