PORT SCANNING - A GENERAL PRIMER

Port scanning - sounds like something from an old science fiction movie where the space captain scans the planet for life. Well, believe it or not, there are elements of truth in that analogy. You see port scanning is the first phase in any attack, especially in well-planned attacks. It is for this reason that you should know a bit about it.

What is it?
Port scanning is what an attacker does against a machine he knows is there or which he suspects to be there. Now how does an attacker know a machine is there? Well there are a couple of ways;

- *ping sweeping* - the attacker knows what your ip is so he sends pings to the full ip range and see which ips respond
- *normal use* - the attacker has visited a website, so he knows that machine is there, or he checks to see where mail for your domain goes by querying your DNS mail exchange record, , or many other normal and legitimate ways.
- *insider knowledge* - the attacker worked for you or has inside contacts and thus knows what servers are available

However it happens the attacker knows, or strongly suspects, that there is a live machine so the question becomes what can he do to the machine in order to gain access or to disrupt it's services. This is where port scanning comes in. For an attacker to try to uncover more information about your machine, they will try to discover what servers or services are running on the machine, they will try to discover what operating system is running on the machine. With port scanning an attacker sends packets to certain ports, or just all of them, in order to see if they respond, and also how they respond. For example, an attacker scans your machine, they get a response from port 25. Hmmm.. thats the SMTP protocol port, could be a mail server or a forgotten service on another type of server. Next they see that that the port responds with a Sendmail response. This response lists the Sendmail version as well. Jackpot, now they know what email server software is running and that it is probably running on a linux box, this means they can focus their attacks more efficiently by trying to exploit weakness in the Sendmail server. The attacker can use a variety of tools for both linux and windows to do this, such as Nmap, Netcat, Superscanner,etc (please see the links page for links to these utilities).

So how does it work?
Well before we go there, lets have a brief overview on the way that a normal tcp session is established, or what is better known as the "three-way handshake";

Sequence	Client	Server
1	Sends SYN packet to server	
2		SYN/ACK packet response to client
3	ACK response sent to server	

After this, the established session carries on as normal. You need to understand this "handshake" process because the way it should work forms the basis many of the different type of port scans. Now lets take a look at the different types of scans;

- *Connect Scan*
  This scan connects to the port and performs a full three-way connection handshake (see above), and is easily detected

- *SYN Scan*
  This scan is also called half-open scanning because a full connection is not made. Just the SYN packet is sent. If the server responds with a SYN/ACK then the port is active. If the server responds with a RST/ACK then the port is closed. This scan is stealthier than a full connection

- *FIN Scan*
  This scan sends a FIN packet to the port, the server should respond with an RST for all closed ports. This technique generally only works against UNIX based TCP/IP stacks.

- *XMAS Tree Scan*
  This scan sends FIN, URG, and PUSH packets to the port, the server should send a RST response packet for all closed ports.

- *NULL Scan*
  This scan turns off all the flags on the packet sent to the port, the server should respond with a RST for all closed ports.

- *ACK Scan*
  This scan sends an ACK packet to the port, and is useful for finding out if the firewall in use is a simple packet filter (which will allow the packet) or a stateful inspection firewall (which will disallow the packet).

- *WINDOWS Scan*
  This scan could detect open and/or filtered ports on some systems due to an exception in how the TCP window size is reported.

- *RPC Scan*
  This scan is used to find and identify an Remote Procedure Call ports and programs. This technique only works against UNIX type systems

- *UDP Scan*
  This scan is used to determine which UDP services are running. A UDP packet is sent to the port, in theory if no response is received than the port is open.

How is this stopped?
Well lets do the bad news first, you see while you can prevent scans, we might not always want to or be able to. You will always want to allow access to your corporate web-server, or corporate email-server. Imposing the restrictions which limit scans on your internal network is not always practical either. The trick is to properly apply the principle of least privilege, you should only allow what is necessary and restrict everything else. The good news is that stateful inspection firewalls stop most of these scans cold, and it is a simple matter to configure rules to only allow proper TCP connections, in fact many of these "sanity-check" rules can even be applied on the server itself, meaning that your protection against scans can be customized as needed depending on the server. And even when you cannot implement these rules, an IDS will be able to monitor and track these scans.

Well thats it. As always I hope it was informative, and helpful. knowing about scanning is important because it could well be the harbinger of a more focused and concentrated attack, so any forewarning will allow for pre-emptive action. Also I would recommend to become familiar with the normal flow of TCP traffic so as recognize and strange patterns. So play, learn and have fun.