Port and Router Vulnerabilities

Welcome back. In this video, we're going to look at some of the vulnerabilities which can be introduced by ports and routers. Accessing a network opens a port and two apps when communicating over a network will we use the same port number. Well-known ports include port 20 and 21 for FTP, 80 for HTTP.

So for example, web browsers talk over port 80. 25 for SMTP. And these are assigned and used by the operating system processes. Port scanning is a process which checks a host's ports, normally the common ones, to see which are open. The data, which comes back from this can be useful for an attacker to identify vulnerabilities in the system. It may be that ports such as file transfer are left open.

And an attacker could then send data through that port. That data could be something like a piece of malware. These scans can also help us identify particular applications and application versions or operating system versions that are being used. Often, there are vulnerabilities related with specific versions of software. And again, this provides an opportunity for an attacker to find a way into a system. Scanning someone's ports can be easier than you might think.

There is software, which you can download to achieve this. A port scanner is a program that sends a request to each of the ports in a list, and notes whether they get a response or not. There are legitimate uses of this, for example, to see particular vulnerabilities such as ports that you might want to close. So as an attacker, if you knew which ports were open, and they are receiving information, then you might be able to do things such as identify utilities which are installed on an operating system. And this could allow you to exploit particular services with known vulnerabilities or send malicious programs and things in on those ports. There are a number of existing software applications to complete these scans. Nmap is a popular open source software which performs them.

Here, we can see the result of a scan which shows the port number followed by the protocol--

all TCP in this example--

then the state of the port, and the service. So just as a health warning, the usual thing--

don't do this on anyone else's machines, only on your own, unless you have formal written legal consent to do so.

When performing router scanning using a tool such as Nmap, there are two general types of scan which can be performed. We have a vanilla scan, which effectively iterates through all the different port numbers and sends a message to determine whether they are open or closed. Or alternatively, we have a stealth scan, or a strobe scan.

A strobe scan, in contrast, is looking for specific services. So it may limit itself to very specific ports. It's important to note that services on these ports may be performing log operations. That is, a scan may log itself as an open request with no data. As a result, of these kind of scans can be identified by the targets, particularly vanilla scans are more prone to this.

Because they work sequentially through each of the ports, it's very likely that somebody would be able to identify that such a scan is taking place. In contrast, a strobe scan is less likely to trigger such an event, because it's more particular about what type of services it accesses. Another thing to consider from an attacker's perspective is the IP address which is being used to perform the scan.

If the same IP address is sending a lot of probes to a range of different ports, then it's very possible that the attacker will be identified. To try and mitigate this, you can look at using things like bot nets or masking your IP address in a different way. Of course, this is not to say that you should actually perform a scan on someone else's computer system or network.

Let's have a look at how a stealth scan or strobe scan works in a little bit more depth. So if someone is port scanning, then they might need more advanced techniques. This is called stealth scanning. And it includes a number of different techniques. One of which is called fragmented packets.

By splitting up the TCP header over several packets, it's harder for packet filters to detect the probe. Let's turn our attention now to routers. As you probably already know, if you're close to a router, it's very likely you'll be able to see that if you have a device which has a wireless card. In particular, if there is no password blocking entry onto that network, then someone could get access to it.

This is called war driving. And you may have seen this if you, at one point, didn't put a passport or some kind of requirement on entry to your network, and noticed perhaps neighbours accessing your network. Clearly this can cause problems, as on occasion, police look for specific online behaviour.

And if that's attached to your network, it would be difficult to make the argument that it wasn't yourself who did this. So it's something to be aware of. As with many things, one of the ways to mitigate this, of course, is to put an appropriate password or other authentication mechanism on to your router so that this stops any unauthorised access to your network. There are of course, other ways of doing this.

For example, if you can add specific MAC addresses. And you can also look at blocking particular IPs. These kind of activities can be executed through your router interface. With IP providers, such as Virgin or BT, they normally have a web interface which allows you to interact with your router.

Why not take some time and explore your own home router to see the kind of configurations that you might put in place. It's important to note that for attacks, such as packet sniffing, you have to be on the same network. So if you're looking at a building or an organisation who has a local area network, an attacker trying to gain access to that would have to get themselves onto that network before they're able to perform packet sniffing activities.

Well, that's us for this video. We've had a look at ports and router vulnerabilities in networks. I hope you enjoyed it, and I'll see you next time.