Server Vulnerabilities

In this video, I'm going to introduce a particular type of server vulnerabilities. These are referred to as denial of service attacks. It's very likely that you've come across a denial of service attack in real life. Effectively, this is where legitimate access is stopped by an attacker. So at a point where a particular system or data should be accessible by the end users, it is no longer the case, because the attacker has managed to stop access.

There are a number of different strategies which an attacker can do to achieve this. We'll cover some of these within this video. But one thing that it's important to point out is that there is always a chance of an unintended denial of service. This happens, for example, where the load on a server is deemed to be excessive compared to what was expected.

As a result, the server can no longer cope with it and access to that particular resource or website, for example, is no longer happening. We've seen examples of this in recent years. When the first new Star Wars film came out, the demand for tickets to the cinema was so large that the ODEON website collapsed under the load. Similarly, in universities, at registration time, we have on occasion seen that the servers crash.

In saying that, let's have a look at some of the different ways an attacker can try and deliver a denial of service attack. The first type of denial of service I'd like to talk about is a service request floods. And that's effectively what we probably see on a more common basis. That could be, for example, with a website HTTP or HTTPS requests. Effectively, the server is overloaded with requests and is unable to deal with them and as a result shuts down.

You can compare this to being within a restaurant. Your waiter comes up and tries to serve you. However, that relies on people waiting their turn. They can serve one person and then move on to the next and manage them as they go. However, if everyone comes at the same time and are all asking the waiter simultaneously to give access to your particular favourite foods, then that server is going to be unable to deal with the load.

And so that is effectively a request flood. Another option is what is referred to as a bandwidth flood. Effectively, this makes use of a specific size or request that a given server can deal with. The attacker constructs a request, which is larger than the bandwidth which the server accepts. And as a result, this can initiate a denial of service.

That's referred to as a bandwidth flood. You can see that there are similarities in terms of the service flood with the bandwidth flood, but where the service requests flood is about the quantity of requests, the bandwidth is about the size of the request. Another type of flood that we're going to cover is the SYN flood. Now this is in the TCP/IP protocol, which includes a handshake. They have to send a send message to the server.

The server has to acknowledge that. And then effectively the client has to acknowledge that response. However, in a SYN flood what happens is that the attacker is going to send loads of requests, open up that handshake multiple times, but they're not going to close off the handshake.

As a result, the server ends up with many open connections, is unable to deal with that, and then potentially turns to denial of service. This is inherent in the way that the TCP/IP operates. And as a result, you can't resolve this issue, unless you violate the protocol design. So clearly, this is a little bit of a problem.

In terms of defending against a denial of service, what we starting to do is to look at security operation centres. These are basically combining a range of different monitoring tools, such as firewalls and demilitarised zones, as well as intrusion detection and prevention systems. They look for key parts, which start to indicate that there might be such an attack either taking place or having taken place. Ideally, we want to try and prevent it.

So using these kind of indicators, it can mean that we can try and stop such an attack happening in the first place. The final point to consider is the distributed denial of service. In the examples that we're discussing, we're probably working on the basis that there's perhaps one attacker using a single machine to do this, but the reality is that often we are using a distributed denial of service.

This means that it's not a single client making those requests or trying to overwhelm the bandwidth. It's multiple clients. One of the ways that the attacker can try to achieve this is to develop a network of what we refer to as zombies. These are computers which have been infected with a bot.

A bot is effectively allowing an attacker to have remote control over that computer. So an individual might be unknowingly contributing to a distributed denial of service attack. A network of zombies is referred to as a bot net. And clearly, this is an example of where you want to ensure that your computers are free of any kind of malware, which might be achieving this.

That's it for this video where we've had a brief overview of denial of service attacks. I hope you've enjoyed that. And I'll see you next time.