NMAP六种端口状态解读

Nmap是一种用来发现网络中主机和服务的安全扫描工具，从而能够产生一个网络“地图”，为了完成这个功能，nmap会向每个目标主机发送特定的报文，从而从目标主机返回报文（或者无返回报文）来判断目标主机的属性（如：开放的端口，所使用的操作系统，操作系统的类型等信息）

本文主要讨论nmap对端口进行扫描中，当nmap向目标主机发送报文并根据返回报文从而认定端口的6种状态的含义（注意：这六种状态只是namp认为的端口状态，例如：有些主机或者防火墙会返回一些不可靠的报文从而妨碍nmap对端口开放问题的确认）。

Open：端口处于开放状态，例如：当nmap使用TCP SYN对目标主机某一范围的端口进行扫描时，我们知道 TCP SYN报文是TCP建立连接的第一步，所以，如果目标主机返回SYN+ACK的报文，我们就认为此端口开放了并且使用了TCP服务。

Closed：端口处于关闭状态。例如：TCP SYN类型的扫描，如果返回RST类型的报文，则端口处于管理状态。这里我们值得注意的是关闭的端口也是可访问的，只是没有上层的服务在监听这个端口，而且，只是在我们扫描的这个时刻为关闭，当我们在另一个时间段进行扫描的时候，这些关闭的端口可能会处于open的状态。

Filtered（过滤的）：由于报文无法到达指定的端口，nmap不能够决定端口的开放状态，这主要是由于网络或者主机安装了一些防火墙所导致的。当nmap收到icmp报文主机不可达报文（例如：type为3，code为13（communication administratively prohibit）报文）或者目标主机无应答，常常会将目标主机的状态设置为filtered。

Unfiltered（未被过滤的），当nmap不能确定端口是否开放的时候所打上的状态，这种状态和filtered的区别在于：unfiltered的端口能被nmap访问，但是nmap根据返回的报文无法确定端口的开放状态，而filtered的端口直接就没就没能够被nmap访问。端口被定义为Unfilterd只会发生在TCP ack扫描类型时当返回RST的报文。而端口被定义为filtered 状态的原因是是报文被防火墙设备，路由器规则，或者防火墙软件拦截，无法送达到端口，这通常表现为发送NMAP的主机收到ICMP报错报文，如：TYPE为3，code为13的报文（通信被认为的禁止 communication administratively prohibited），或者主机通过多次重复发送没有收到任何回应）。

 Open|filtered状态，这种状态主要是nmap无法区别端口处于open状态还是filtered状态。这种状态只会出现在open端口对报文不做回应的扫描类型中，如：udp，ip protocol ，TCP null，fin，和xmas扫描类型。

  Closed|filtered状态，这种状态主要出现在nmap无法区分端口处于closed还是filtered时。此状态只会出现在IP ID idle scan（这个类型我现在也不太理解，过段时间进行总结一些）中。