DHCP 的攻击有哪些？有什么防护手段

1.刚开始看到理论题的时候有点懵，考官人不错，在自我介绍前给了我几分钟做准备，所以我就想了一下理论题，发现跟 DHCP snooping 差不多，所以我讲理论的时候就按照讲 DHCP snooping 的套路讲了，全程讲的时候考官都没打断我

追问 1：DHCP 是基于什么封装的？
答：我当时没想到，因为 DHCP 是特性那块，没怎么认真看，当时答了是基于 2 层（其实是基于 UDP）。DHCP Server 使用端口号 67 来接收 DHCP 消息，DHCP Client 使用端口号 68 来接收 DHCP 消息

追问 2：如果一个客户端隔了一个广播域怎么获取到地址？
答：这个我说了通过 DHCP 中继去获取。然后问我中继的工作过程，我没复习到，在那卡了一会。然后考官就问下一个问题

追问 3：DHCP snooping 绑定表有动态和静态，那么静态的绑定表怎么实现？
答：当时我就觉得应该是如何配置命令，但我没试过静态绑定，所以就说没做过静态，只做过动态，而动态就是通过监听服务器和客户端的报文来自动生成表项的。

追问 4：DHCP 报文泛洪攻击都泛洪什么报文？
答：我就说有 Report、Inform、Release、Discover、Dcline 报文，通过配置对 DHCP 报文处理单元检测防护。考官就问 Release 报文不会被速率限制那怎么办，当时脑子一懵就说了绑定表出来，绕了几分钟这个问题。后来考官就说下一题，没有追问下去