请描述 IP 分片污染攻击的原理与攻击者需要具备的能力

1. IP 分片污染攻击的基本原理

IP 分片是一种位于网络层的机制，其主要目的是解决 IP 分组在不同最大传输单元（MTU）网络中的传输问题。然而，在某些情况下，网络层的 IP 分片机制可能会被攻击者利用来破坏和污染原始的网络数据流。如果攻击者能够被动地监视，或者主动触发源主机和目标主机之间的IP分片，那么攻击者就有可能伪装成源主机，制造恶意的 IP 分片，并将其注入源主机和目标主机之间的数据流中，从而污染原始流量，对目标主机进行攻击。

2. 攻击者需要的能力

攻击者需要具备伪造 IP 地址的能力，因为他们需要假冒源主机来发送伪造的 IP 分片。此外，攻击者还需要能够预测源主机分配的 IPID，因为接收端是根据 IPID 来重新组合分片的，而在许多系统中，IPID 是可以预测的。

结合几个针对 DNS 域名服务实施的 DDoS 攻击案例分析提升 DDoS 攻击防御能力的可行措施

分析案例

DNS请求洪水攻击

DNS请求洪水攻击是一种攻击手段，其中黑客通过控制僵尸网络向DNS服务器发送大量不存在的域名解析请求，最终导致服务器因处理大量DNS请求而超载，无法继续响应正常用户的DNS请求，从而实现攻击目标。在这种攻击中，攻击源可能是虚假的，也可能是真实的；攻击目标可能是DNS授权服务器，也可能是DNS缓存服务器。因此，针对不同类型的攻击源，需要采取不同的防御策略。

DNS回应洪水攻击

在DNS回应洪水攻击中，黑客发送大量的DNS回应报文到DNS缓存服务器，导致缓存服务器因处理这些DNS回应报文而耗尽资源，影响正常业务的过程。大多数DNS回应洪水攻击都是虚假源攻击，黑客控制的僵尸主机发出的DNS回应报文的源IP地址通常都是伪造的，是不存在的。因此，在防御时，可以从回应源IP地址的真实性进行判断。

防御策略

TC源认证

DNS查询有TCP和UDP两种方式。通常情况下，DNS查询都是基于UDP的，此时TC标志位为0。可以通过将TC标志位设置为1来将UDP改为TCP方式。当DNS请求报文的速率超过阈值时，启动源认证机制：拦截DNS请求，将TC标志位设置为1并进行回应，要求客户端以TCP方式重新发起DNS查询。如果源是虚假的，则系统不会正常响应这个DNS回应报文，更不会通过TCP方式重新进行DNS查询。如果是真实客户端发送的请求，则系统会重新发送SYN报文，请求建立3次握手。源认证通过后，客户端源IP地址被加入白名单。客户端重新请求建立3次握手，系统将客户端第2次发送的3次握手请求直接放行，发送给服务器。客户端与服务器之间建立3次握手成功，并通过TCP方式完成本次DNS查询。

被动防御

被动防御模式利用DNS的重传机制，不反弹DNS查询报文，而是直接丢弃，然后看客户端是否重传。当客户端发送的DNS请求报文速率超过告警阈值后，启动源认证机制：在第一次收到DNS请求报文后，记录DNS请求报文的域名、源IP地址等基本信息生成的HASH值，并丢弃首包。后续

一定时间内，如果系统再收到与这个HASH值相同的DNS请求报文时，就认定其为重传包，对其执行放行操作。

限速防御

可以采用域名限速和源IP地址限速，针对DNS请求报文和DNS回应报文都生效。

- 如果某个域名的DNS请求或回应报文速率过高，我们可以针对这个域名进行限速。通常某个域名遭受的访问量一直高，但突然有一天某访问量增长到平时的很多倍，此时我们可判断这个域名可能遭受了攻击。针对性地对某个特定域名进行限速，而不影响其他域名的正常请求。
- 如果某个源IP地址域名解析的速率过大，源IP地址限速就可以有针对性地限速这个源IP地址的DNS请求报文或者DNS回应报文，这样也不会对其他源造成影响。