Idle Scan

**1.简介**

它允许进行完全盲目的端口扫描。事实上，攻击者可以不用向目标发送数据包就完成扫描工作！相反，用猥琐的边信道攻击是能够让扫描映射到一个Zombie主机上的。除了极其隐蔽的情况，这种扫描方式允许挖掘机器之间基于IP的信任关系。

**2.工作流程**

（1）确认TCP端口已经打开，并且向这个端口发送一个SYN（建立了会话）包。如果端口是开放的，目标机器会返回一个SYN/ACK包响应。如果端口没开放，那我们只有另辟蹊径咯

1. .机器接受一个未经请求的SYN/ACK包会返回RST，一个未经请求的RST会被忽略。

（3）.任何数据包在互联网上都有一个片段标识号（IP ID），当数据包发送的时候，许多操作系统只是简单的增加了数字，未做其他处理。所以攻击者只需要探究IPID就可以知道最终发送了多少个包。





