名词解释

1. **异常检测技术**
   异常检测的假设是任何一种入侵行为都能由于其偏离正常或所期望的系统和用户的活动规律而被检测出来
2. **误用检测（滥用检测）**
   一种基于模式匹配的网络入侵检测技术，将搜集到的信息与已知的网络入侵和系统误用模式数据库进行比较，即可发现未知的网络攻击行为
3. **TCP 半连接**
   在三次握手过程中，服务器发送 SYN-ACK 之后，收到客户端的 ACK 之前的 TCP 连接称为半连接
4. **VPN**
   是公司内部或者不同公司和组织之间为了在广域网上进行通信而建立的私有通信网络
5. **DMZ（非军事化区）**
   为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区
6. **僵尸网络**
   计算机被病毒感染后，随时按照黑客的指令展开拒绝服务攻击或发送垃圾信息，（用户毫不知情，仿佛没有自主意识的僵尸）这样的计算机达到一定数量后，形成一个庞大的网络
7. **泪滴攻击**
   IP 数据包在网络传递时，数据包可以分成更小的片段，攻击者可以通过发送两端或更多数据包实现泪滴攻击
8. **IP 地址欺骗**
   攻击者假冒他人 IP 地址，发送数据包
9. **交换机失败保护模式**
   交换机所处特殊模式，交换机维护 IP 地址和 MAC 地址的映射关系时会花费一定处理能力，网络通信出现大量虚假 MAC 地址时，某些类型的交换机会出现过载情况，从而转化到失败保护模式，工作方式和集线器相同
10. **零日漏洞**
    指被发现后立即被恶意利用的安全漏洞，能造成巨大破坏
11. **木桶理论**
    整个系统防护能力，取决于系统中安全防护能力最薄弱的环节
12. **DDOS 攻击**
    是目前企业网络和电信网系统面临最主要攻击类型之一，要么大数据、大流量压垮网络设备和服务器，要么有意制造大量无法完成的不完全请求来快速耗尽服务器资源
13. **TCP SYN 扫描**
    通常是“半开放扫描，扫描端收到 ACK/SYN 应答时，发送了一条拒绝建立连接的 RST 请求，目标端不会将其记录在日志中”