根据之前学过的内容我们可以知道，攻击者可以通过开源工具和技术获得大量关于基础设置的敏感信息。作为渗透测试者，我们不能只关注如何攻击一个网络，我们还要理解如何缓解这些问题，给客户合理的建议和指导。企业可以采取几种方法让攻击者在实施一次隐蔽、成功的攻击并获取所需要的信息时变得困难。

1. 命名规则

应该鼓励管理员使用不暴露设备信息的名字。（推荐使用内部命名规范，让入侵者难以理解，而合法的管理员却能够立刻了解每台服务器的功能）

1. Port Knocking技术

管理员通常使用Port Knocking技术以避免端口扫描。这个概念非常简单，需要在连接某个管理端口前（如SSH），首先连接一个秘密开放的端口

Port Knocking更高级的用法是建立一个Telnet服务器，如果有IP尝试连接Telnet端口，则基于主机的防火墙临时阻断对系统任何端口的访问。



1. 入侵检测和规避系统

尽管这些系统不像厂商宣传的那样能够提供完美的安全服务，但是一个正确配置的入侵检测系统（基于主机或者基于网络）对检测扫描有很大的帮助。这些设备应该用作公司深度防火策略的一部分，需要进行正确的管理、监控和更新，这样有助于解决公司面临的安全问题。

1. 触发点

策略性地设置一些早期预警系统，当有访问的时候就发出警告，类似物理安全中的边界入侵检测。管理员应该规避在系统上开放尽可能多的端口，因为这会改变系统的主要用途。值得注意的是，如果网络中存在这样的系统，它应该与网络上其他系统一样经常得到维护。没有打补丁的系统无疑是攻击者的首选目标，无论如何，让攻击者在网络中获得一个立足点绝对不是一个好的主意。一旦攻击者找到内网扩展的支点，他们的工作就会变得更加简单，到时候尽管你响应了触发的预警系统，攻击者可能已经在网络中其他系统上留下了后门程序。

1. 关闭SNMP

确保管理员以安全的方式使用SNMP。SNMP可以让攻击者获得大量有价值的信息。建议SNMP使用最新的安全策略，阻断和限制访问SNMP主机，最重要的是移除默认的团体名public。（由于各种原因，客户有可能不能使用最新的SNMP版本。在这种情况下，应尽可能地维护协议的安全性。如：应该锁定特定的主机访问SNMP）