SSH（Secure Shell）安全外壳协议，建立在应用层基础上的安全协议；专为远程登录和其他网络服务提供安全性的协议。防止远程管理过程中的信息泄露问题；ssh传输数据是加密和压缩的。SSH的组成：

传输层协议

用户认证协议

连接协议

SSH两种级别验证方法

基于口令的安全验证：用账户和口令就可以登录到远程主机，传输的数据是加密的但是不一定连接到你想连接的服务器，容易受到MITM攻击

基于秘钥的安全验证：可以防止MITM攻击