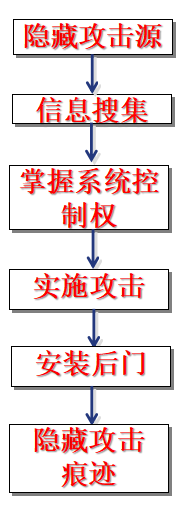
1. 网络攻击一般步骤



1. 网络攻击三部曲——信息收集技术、攻击实施技术、隐身巩固技术

A.信息收集技术主要技术：网络踩点、网络扫描、网络监听

B.攻击实施技术主要技术：社会工程学攻击、口令攻击、漏洞攻击、欺骗攻击、拒绝服务攻击

C.隐身巩固技术主要技术：设置代理跳板、清除日志、留后门

1. 拒绝服务攻击（DOS）（Denial of Service）

基本概念：拒绝服务攻击的主要目的是使被攻击服务器资源耗尽或系统崩溃而无法提供服务。

基本方式：最基本的DoS攻击利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务器的响应。

DoS攻击类型：a.带宽耗用DoS攻击。b.资源衰竭DoS攻击。c.编程缺陷DoS攻击。

d.基于路由的DoS攻击。e.基于DNS的DoS攻击。

1. 分布式拒绝服务（DDOS： Distributed Denial of Service ）

基本概念：DDOS是一种基于DoS的特殊形式的拒绝服务攻击，是一种分布、协作的大规模攻击方式。

与DOS的不同：DoS攻击只要一台单机和一个modem就可实现，与之不同的是DDoS攻击是利用一批受控制的机器向一台机器发起攻击，这样来势迅猛的攻击令人难以防备，因此具有较大的破坏性。

特点：不可预测和持久性。

主要分类：1.UDP洪水攻击：a.DNS反射攻击。b.网络时间协议（NTP）反射攻击。

c.简单服务发现协议（SSDP）反射攻击。2.TCP洪水攻击。...  
5.APT攻击

定义：可以从“A”、“P”、“T”三个方面来理解NIST对APT的定义:1）A（Advanced）：技术高级。2）P（Persistent）：持续时间长。3）T（Threat）：威胁性大。

APT攻击的两个显著特点：1）目标明确2）手段多样