# 工控安全仿真沙盘（仿真实验室）

随着计算机和通信技术的飞速发展，对安全的高速网络数据传输协议的需求不断加强，随之出现了许多网络仿真工具。目前，国内外已经出现了很多关于网络仿真的工具，一般这些工具的针对性很强。比如Cnet是一种网络协议模拟器，它突出强调TCP/IP网络协议的仿真，可以在由点对点连接IEEE 802.3以太段组成的网络中对各种数据链路层、网络层、路由和传输层的网络协议进行实验性的模拟。OPNET是一个强大的协议仿真工具，为协议仿真提供了一个良好的环境，但是丁过于复杂，光要熟悉这个环境就需要花费很长时间。

仿真技术的发展先后经历了发展、成熟、高级三个阶段和分布式仿真DS、分布式交互仿真DIS、聚合级仿真协议ALSP、高层体系结构HLA四个时期。在此期间，一些国外研究机构对网络安全仿真进行了卓有成效的研究，研发了多个网络安全仿真平台（测试床）。比如，美国犹他大学开发的互联网仿真系统Emulab，后期发展为网络综合测试床Netbed，Emulab/Netbed致力于创建包含模拟、仿真和广域网测试床等多种试验环境的开放综合框架，并能够通过统一的用户界面对试验条件进行灵活配置。DETER计划是由美国国家科学基金（NSF）和国土安全高级研究开发计划署（HSARPA）联合研制幵发的大型综合试验床，目标是创建、维护和支持一个协作和中立的计算机网络仿真环境，使研究者能够直观方便地分析、评估各种网络行为，尤其是对网络攻防的测试与评估，DETER计划也是网络建模与仿真方面最有影响的项目。DETER还有一个姐妹计划EMIST（因特网安全技术评估方法），其目标是开发针对特定类型网络攻击的、严密的、符合实际的测试框架、分析方法及相应的防卫机制，它实际上是一个由多个半实物试验床组合而成的综合仿真环境。另外一个比较有影响的项目是安全和系统建模项目其关注的主要问题是大规模网络系统安全性仿真，并己成功对DDOS攻击、蠕虫传播以及BGP攻击等安全问题进行了仿真。然而，由于保密等因素，相关研究资料难以获得。除了这些大型网络安全仿真系统之外，一些研究者还利用仿真工具对具体的网络安全问题（如DDOS攻击、 入侵检测算法等）进行了探索，其中具有代表性的有：

1）佛罗里达大学的Shabana Razak等人在使用OPENT搭建的网络环境中将流量文件 收集的各种攻击数据在仿真环境中进行了重现，并使用这些模拟的攻击数据包对一种基于特征的入侵检测算法进行了验证。

2）土耳其SABANCI大学的五名学者针对DSR ad hoc路由协议在OPNET中建立了攻击模型并分析了攻击模型对DSR路由发现机制的攻击效果。

与国外相比，国内研究相对滞后，一定程度上还处于学习和模仿阶段。近年来，随着网络安全问题的日益突出和美国解除高端网络仿真软件出口的限制，我国一些大学和科研机构也对网络安全仿真领域进行了探索，并取得了一些成果。

1）中科院在2005年基于NS2开发了一个网络安全建模环境以支持对网络安全技术和可生存系统架构的研究和验证，并成功运用该平台对蠕虫传播进行了较逼真的模拟。

2）西安电子科技大学开发了一个基于口Linux的网络攻防模拟平台，主要面向大学计 算机网络和信息安全课程的教学需要。

# 工控攻击方法

## 口令窃取

登录一台计算机的最容易的方法就是采用口令进入。口令窃取一直是网络 安全上的一个重要问题，口令的泄露往往意味着整个系统的防护已经被瓦解。

如果系统管理员在选择主机系统时不小心的话，攻击者要窃取口令文件就将易如反掌。口令猜测是使用最多的攻击方法，即利用字典或穷举方法把登录口令给找出来。

## 缺陷和后门

事实上没有完美无缺的代码，也许系统的某处正潜伏着重大的缺陷或者后门，等待人们的发现，区别只是在于谁先发现它。只要本着怀疑一切的态度，从各个方面检查所输入信息的正确性，还是可以回避这些缺陷的。比如说，如果程序有固定尺寸的缓冲区，无论是什么类型，一定要保证它不溢出；如果使用动态内存分配，一定要为内存或文件系统的耗尽作好准备，并且及时释放分配的内存。

## 鉴别失败和协议失败

即使是一个完善的机制在某些特定的情况下也会被攻破。如果源机器是不可信的，基于地址的鉴别也会失效。一个源地址有效性的验证机制，在某些应用场合能够发挥作用，但是黑客可以用程序Portmapper重传某一请求。在这一情况下，服务器最终受到欺骗。对于这些服务器来说，报文表面上源于本地，但实际上却源于其他地方。寻找协议漏洞的游戏一直在黑客中长盛不衰，在密码学的领域尤其如此。有时是由于密码生成者犯了错误，过于明了和简单。更多的情况是由于同的假设造成的，而证明密码交换的正确性是很困难的事。

## 信息泄漏

信息泄露是指信息被泄露或透露给某个非授权的实体。大多数的协议都会泄漏某些信息。高明的黑客并不需要知道局域网中有哪些计算机存在，他们只 要通过地址空间和端口扫描，就能寻找到隐藏的主机和感兴趣的服务。最好的防御方法是高性能的防火墙，如果黑客们不能向每一台机器发送数据包，该机器就不容易被入侵。

## 病毒和木马

所谓计算机病毒，是一种在计算机系统运行过程中能够实现传染和侵害功能的程序。一种病毒通常含有两种功能：一种功能是对其他程序产生“感染"； 另外一种或者是引发损坏功能，或者是一种植入攻击的能力。蠕虫病毒是最近几年才流行起来的一种计算机病毒，由于它与以前出现的计算机病毒在机理上 有很大的不同(与网络结合)，一般把非蠕虫病毒叫做传统病毒；把蠕虫病毒简称为蠕虫。随着网络化的普及，特别是Internet的发展，大大加速了病毒的传播。

“特洛伊木马”(Trojan horse)简称“木马"，完整的木马程序一般由两个 部分组成：一个是服务器程序，一个是控制器程序。对于木马来说，被控制端 是一台服务器，控制端则是一台客户机。黑客经常引诱目标对象运行服务器端程序，这一般需要使用欺骗性手段，而网上新手则很容易上当。黑客一旦成功 地侵入了用户的计算机，就会在计算机系统中隐藏一个会在Windows启动时悄 悄自动运行的程序，采用服务器／客户机的运行方式，从而达到在用户上网时 控制用户的计算机的目的。计算机病毒和木马的潜在破坏力极大，正逐步成为 信息战中的一种新式进攻武器。

## 欺骗攻击

网络欺骗攻击作为一种非常专业化的攻击手段，给网络安全管理者带来了严峻的考验．主要方式有：IP欺骗、ARP欺骗、DNS欺骗、Web欺骗、电子邮件欺骗、源路由欺骗(通过指定路由，以假冒身份与其他主机进行合法通信 或发送假报文，使受攻击主机出现错误动作)、地址欺骗(包括伪造源地址和伪造中间站点)、非技术类欺骗(利用人与人之间的交往，通常以交谈、欺骗、假 冒或口语等方式，从合法用户中套取用户系统的秘密)等。

## 拒绝服务

DoS攻击，其全称为Denial ofService，又被称为拒绝服务攻击。直观地说，就是攻击 者过多地占用系统资源直到系统繁忙、超载而无法处理正常的工作，甚至导致 被攻击的主机系统崩溃。攻击者的目的很明确，即通过攻击使系统无法继续为合法的用户提供服务。网络攻击的方法的分类有多种，如基于攻击效果可以分 为破坏、泄露和拒绝服务等。还可以把对安全性的

攻击分为两类：被动攻击和主动攻击。被动攻击试图获得或利用系统的信息，但并不会对系统的资源造成 破坏，如窃听和监测；主动攻击则试图破坏系统的资源，并影响系统的正常工作，如拒绝服务等。