第 16 卷第 4 期,增刊　　广西科学院学报　　Vol. 16, No. 4 & Supplement
2000 年 11 月　　Journal of Guangxi Academy of Sciences　　November 2000

网络战中的网络欺骗技术
Network-cheating in Network War

许泽平　　伍文海
Xu Zeping　　Wu Wenhai

(桂林陆军学院　桂林　541006)
(Guilin Military College, Guilin, 541006)

摘要　简述网络欺骗的概念、作用以及主要的欺骗技术，如 Honey Pot、欺骗空间、技术网络流量仿真、多重地址转换、网络动态配置和创建欺骗信息。

关键词　网络伪装　网络欺骗　Honey Pot　欺骗空间　技术网络流量仿真　多重地址转换　网络动态配置

中图法分类号　TP 393.08

Abstract　The definition of network-cheat and its functions in protection of network are described. The techniques of network-cheating such as Honey Pot, cheating space, network flow simulation, multiple address translation, network dynamic configuration and creating false information are introduced.

Key words　network-mask, network-cheat, Honey Pot, cheating space, network flow simulation, multiple address translation, network dynamic configuration

信息战是新生的作战样式，计算机网络技术则是支撑信息战的主要核心技术。由计算机网络技术发展而引起的计算机网络安全问题，开辟了军事战争领域的又一空间，即基于网络技术的网络战。现在世界各军事强国都在发展网络技术，抢先占有制网络权。通过网络方式将病毒植入敌方计算机主机、网络设备以伺机破坏敌方的指挥控制系统、通信系统等高敏感的网络系统；或者通过网络窃取或恶意破坏敌方机要数据等。在网络进攻和反进攻的相互促进发展中，网络欺骗技术正成为人们的研究焦点。

1　网络欺骗的概念

网络欺骗就是通过布置网络陷阱，使入侵者相信信息系统存在有价值的、可利用的安全弱点，并具有一些可攻击窃取的资源（为吸引入侵者伪造的或并不是重要的资源），将入侵者引向这些错误的资源，从而显著地增加入侵者的工作量、入侵复杂度以及不确定性，使入侵者难以判断其进攻是否奏效或成功，同时，它允许防护者跟踪入侵者的行为，在入侵者攻击之前修补系统可能存在的安全漏洞，以更好的保护自己的系统，并能在适当时机对入侵方进行致命的反击。

2　网络欺骗的作用

从理论上讲，每个有价值的网络系统都存在安全弱点，而且这些弱点正是入侵者突破网

2000-08-27 收稿。

络系统的入口。一个成功的网络欺骗所设置的网络陷阱（伪装弱点）可以使入侵者感到他们达到期望的目标（当然目标是假的）并不容易，并相信其入侵取得了成功。由此可见，网络欺骗有 3 个作用：一是误导入侵者，使其按照我方的意志进行“选择入侵”，进入我方预先设置的网络陷阱；二是通过网络探测，迅速地检测到入侵者的进攻企图，及时修补系统可能存在的安全漏洞，并获知敌方的进攻技术和意图；三是通过与入侵者的周旋，消耗入侵者的资源，伺机反击。

3 网络欺骗的主要技术

3.1 Honey Pot 和分布式 Honey Pot 网络欺骗

Honey Pot 就是为了诱导入侵者而设置的具有吸引力的伪造目标，即欺骗。Honey Pot 和分布式 Honey Pot 网络欺骗是通过隐藏和安插错误信息等技术手段实现，前者包括隐藏服务、多路径和维护安全状态信息机密性，后者包括重定向路由、伪造假信息和设置圈套等等。

最早采用的网络欺骗是 Honey Pot 技术，它将少量的 Honey Pot 置于入侵者很容易发现的地方，以诱使入侵者上当。这种技术的目标是寻找一种有效的方法来影响入侵者，使得入侵者将技术、精力集中到 Honey Pot 而不是其它真正有价值的正常系统和资源中。Honey Pot 技术还可以做到一旦入侵企图被检测到时，就能将入侵者迅速地切换到 Honey Pot。但是，对稍高级的网络入侵，Honey Pot 技术就作用甚微了。因此，分布式 Honey Pot 技术便应运而生，它将 Honey Pot 散布到网络的正常系统和资源中，利用闲置的服务端口来充当欺骗，增强网络的欺骗性，增大入侵者遭遇欺骗的可能。它有 2 个直接效果：一是将欺骗分布到更广范围的 IP 地址和端口空间中；二是增大欺骗在整个网络中的百分比，使得欺骗比安全弱点被入侵者扫描器发现的可能性增大。

尽管如此，分布式 Honey Pot 技术也不是完美的，它仍具有局限性，体现在：一是它对穷尽整个空间搜索的网络扫描无效；二是只提供了相对较低的欺骗质量；三是只相对使整个搜索空间的安全弱点减少；四是它只对远程扫描有效，也就是说，如果入侵已经部分进入到网络系统中，处于观察（如嗅探）而非主动扫描阶段时，真正的网络服务对入侵者已经透明，那么这种欺骗将毫无意义。

由此可见，随着网络战手段的不断提高，仅使用一种网络欺骗技术来进行网络伪装，肯定难以成功。只有不断地提高欺骗质量，才能使入侵者难以将合法服务和欺骗区分开来。因此，还要使用欺骗空间技术、网络流量仿真技术、网络动态配置技术、多重地址转换技术和组织信息欺骗技术来有效增强网络欺骗的质量，提高网络欺骗的成功率。

3.2 欺骗空间技术

欺骗空间技术就是通过增加搜索空间来显著地增加入侵者的工作量，从而达到安全防护的目的。其原理是，利用计算机系统的多宿主能力，在只有一块以太网卡的计算机上实现具有众多 IP 地址的主机，而且每个 IP 地址还具有它们自己的 MAC 地址。利用这项技术，只要极低的花费就可建立一大段欺骗的地址空间。事实上，现在已有研究机构能将超过 4000 个 IP 地址绑定在一台运行 Linux 的计算机上。这意味着利用 16 台计算机组成的网络系统，就可做到覆盖整个 B 类地址空间的欺骗。可见，许许多多不同的欺骗，只需 1 台计算机就可实现。

从欺骗效果上看，将网络服务和网络欺骗分散放置在所有这些 IP 地址上将毫无疑问地增加了入侵者的工作量，因为他们需要判断其中哪些服务是真的，哪些服务是伪造的。而且，在

这种情况下，欺骗服务相对于真正服务更容易被扫描器发现，通过诱惑使入侵者上当，增加入侵时间，消耗入侵者的资源，使真正的网络服务被探测到的可能性大大减小。当入侵者的扫描器访问到网络系统的外部路由器并探测到一欺骗服务时，还可将扫描器所有的网络流量重定向到欺骗上，使得接下来的远程访问成为这个欺骗的继续。值得注意的是，采用这种欺骗时，网络流量和服务的重定向必须严格保密。一旦暴露，就会招致入侵者攻击，从而导致入侵者很容易将任一已知有效的服务和这种用于测试入侵者的扫描探测及其响应的欺骗区分开来。

3.3　网络流量仿真

网络流量仿真是指通过技术手段，使欺骗系统产生与真实网络系统仿真的网络流量，提高网络欺骗质量，使得通过流量分析不能分辨欺骗系统与真实系统。在欺骗系统中产生仿真流量有 2 种方法：一是采用实时方式或重现方式复制真正的网络流量到欺骗系统，这使得欺骗系统与真实系统十分相似，因为所有的访问连接也都被同时复制了；二是从远程产生伪造流量，使入侵者可以发现和利用。

3.4　多重地址转换

多重地址转换就是重定向代理服务，由代理服务进行地址转换，使相同的源地址和目的地址像真实系统那样被维护在欺骗系统中。多重地址转换可利用真实的计算机替换低可信度的欺骗，增加了间接性和隐蔽性，并且，还可将欺骗服务绑定在与提供真实服务主机相同类型和配置的主机上，从而提高欺骗的真实性。

3.5　网络动态配置

实际上，真实网络总是随时间而动态变化的，如果欺骗是静态的，那么在入侵者长期监视的情况下欺骗就非常容易暴露。因此，必须动态地配置欺骗网络来模拟正常的网络行为，使得欺骗网络也像真实网络那样随时间而动态变化。为了使欺骗网络动态配置有效，还须使欺骗具有真实系统的一些特性。例如，办公室的计算机在下班之后关机，那么欺骗计算机也应该在同一时刻关机。另外，假期、周末和特殊时刻也须考虑，否则入侵者将很可能发现欺骗。

3.6　创建欺骗信息

假设某一系统对内部提供了有关某部队人员和武器装备信息的访问服务，那么欺骗也必须以某种方式反映出这些信息。例如，如果系统的分布式网络服务服务器包含了各级首长机关人员的详细信息，那么你就需要在欺骗的分布式网络服务服务器列表中创建欺骗的同类信息，否则欺骗就很容易被发现。这里还要求，伪造的人员也必须要有伪造的信息如职务、级别和个人简历等等。

4　结语

高质量的伪装在传统战法中起着重要作用，而网络欺骗在网络攻击和安全防护中同样有着不可替代的优势，它使得可能存在的安全弱点有了很好的隐藏伪装场所，真实服务与欺骗服务几乎融为一体，使入侵者难以区分。因此，今后的网络战绝对离不开网络伪装。要想取得制网络权，就必须掌握最前沿的网络欺骗技术，谁抢占了网络战的技术优势，谁就能在未来的网络战中立于不败之地。

（责任编辑：蒋汉明）