黑客入侵技术详解:cisco路由入侵艺术思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E9_BB_91_E5_AE_A2_E5_85_A5_E4_c101_644232.htm 奔流不息的网络里，Web绽放着绚丽的色彩、电子邮件呼哧的穿梭网际、语音电话、网络会议、文件传输，各种数据交织错落，形成辉煌的数字世界。在喧闹的数字世界底层，存在一种精致的次序，这种次序决定着数据的选路、异构介质衔接、协议的交互等功能。而这一次序的缔造者正是布满整个网络的路由器。于是，路由器成了数据通信的交通亭，也成为了众多黑帽(Blackhat)争夺的目标之一。 Cisco路由器占据这网络世界的绝对位置，于是安全焦点效应激发了路由入侵与防御而产生的精美艺术。下面我将由浅入深的方式讲述Cisco入侵的手段以及防御策略。 【路由器感冒】 路由器从本身的IOS来说，并不是一个健壮的体系，因而它偶尔也会让自己感冒发烧。系统感冒发烧起来，抵抗力自然就降低不少。 *IOS自身欺骗 Cisco路由器是用IOS系统来实现路由的细节功能，因此它是路由系统的灵魂。Show命令的在线系统方式却为我们打开一个偷窥之门。 众所周知，Cisco路由器中，一般用户只能查看路由器的很少信息。而能进入特权模式的用户才有资格查看全部信息和修改路由。一般模式下，show的在线帮助系统不会列表所有可用的命令，虽然75个show的扩展参数只能用于特权模式下(enable)，实际上只有13个受到限制。这意味着一般用户(非特权用户)可以查看访问列表或其他路由安全相关信息。 重要安全相关的ACL信息可以被登录路由的非特权用户查看，诸如： #show access-lists #show ip prot #show ip ospf dat

#sh ip eigrp top 等命令可以在非特权模式下泄露网络敏感信息。通过这些命令，我们能得出路由器配置的大致情况，这对采取进一步的入侵起到辅助作用。不过由于这种方式需要用户已经有一个登录帐户，因此得到这样的信息有一定难度。*WCCP暗道 Cisco在IOS 11.2版本中引入WCCP(Web Cache Control Protocol)，为Cisco缓存引擎提供协议通信。Cisco缓存引擎为www提供透明缓存服务。缓存引擎用WCCP来和其他cisco路由器通信。路由器把HTTP数据发送到缓存引擎主机中。 虽然这种方式默认是关闭的。假如使能(enable)的话，那么WCCP本身是没有认证机制的。路由器将会把每一个发送合法缓存引擎类型的Hello包的主机认为缓存引擎，于是把HTTP数据缓存到那台主机。这意味着恶意用户可以通过这种方式获取信息。 通过这种方式，攻击者可以截获站点认证信息，包括站点密码；替代实际WEB内容为自己设计的陷阱；通过路由彻底破坏Web提供的服务。这种方式，可以完全规避登录烦琐的攻击方法，对Web提供全面而且致命的打击。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com