黑客WEB攻击新动向：劫持域名换手法思科认证 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_A2WEB_E6_c101_644177.htm 近期发现adobe com,internet.com,nike.com,等等着名站点都分分遭受到攻击，但攻击者所使用的技术并不是以往所使用的入侵WEB服务器，更改主页的惯用手法，攻击者使用的是一种域名劫持攻击技术，攻击者通过冒充原域名拥有者以E-MAIL方式修改网络解决方案公司的注册域名记录，将域名转让到另一团体，通过在修改后注册信息所指定的DNS服务器加进该域名记录，让原域名指向另一IP的服务器，通常那两台服务器都是攻击者预先入侵控制的服务器，并不归攻击者所拥有。百考试题论坛 那攻击者到底是怎样实施该域名劫持攻击的呢？从攻击者的过程来看，主要有5个步骤： 1.获得要劫持的域名注册信息 攻击者会先访问网络解决方案公司www.networksolutions.com,通过该公司主页面所提供的MAKE CHANGES功能，输入要查询的域名，获得该域名注册信息。并通过相关的攻击手段，获取更多的关于该网站的安全资料。本文来源:百考试题网 2.控制该管理域名的E-MAIL帐号 从上面获得的信息，攻击者可了解到abc.com的注册DNS服务器，管理域名的E-MAIL帐号，技术联系E-MAIL帐号等等注册资料，攻击者的重点就是先需要把该管理域名的E-MAIL帐号abc.legal.internet.registration@ABC.COM控制，进行收发在网络 解决方案公司networksolutions主页所修改域名注册记录后的确认E-MAIL,对该E-MAIL帐号的控制过程不排除攻击者对

该E-MAIL帐号进行密码暴力猜测，对该帐号所在E-MAIL服务器进行入侵攻击。 3.修改该域名在网络解决方案公司的注册信息 到这个时候，攻击者会使用网络解决方案公司networksolutions的MAKE CHANGES功能修改该域名的注册信息，包括拥有者信息，DNS服务器信息，等等。 4.冒充拥有者使用管理域名的E-MAIL帐号收发网络解决方案公司确认函 攻击者会在该管理域名E-MAIL帐号的真正拥有者收到网络解决方案公司确认函之前，把该E-MAIL帐号的信件接收，使用该E-MAIL帐号回复网络解决方案公司进行确认，进行二次回复确认后，将收到网络解决方案公司发来的成功修改注册记录函，攻击者成功劫持域名。来源：考试大的美女编辑们 5.在新指定的DNS服务器加进该域名记录 在注册信息新指定DNS服务器里加进该域名的PTR记录，指向另一IP的服务器，通常那两台服务器都是攻击者预先入侵控制的服务器，并不归攻击者所拥有。 编辑特别推荐: 关于思科认证考试的注意事项 各个方向CCIE认证投资回报分析 思科证书的意义：技术经验的证明 我是主考官：给一位应届毕业生的回信 