思科认证辅导:新安全密码规则思科认证 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__E6_80_9D_E7_A7_91_E8_AE_A4_E8_c101_644238.htm 大多数公司都有某种形式的密码政策，这些规则基本上一成不变，即使面对不同的情况、不同的文化或者新型技术：* 不要将密码写下来 * 选择较长的、复杂的密码 *不要保存密码在浏览器 绝大部分安全系统仍然依赖于这种方式：用户名/密码对。在现在这个随时随地都可以接入网络的时代，键盘记录器和木马的存在，这些规则方法还有意义吗?如果仍然使用以上规则，我们是否能够依赖于用户名/密码?答案是否定的。来源：考试大的美女编辑们 让我们面对现实：当键盘记录器出现的时候，基于密码的安全保护就已经过时了。在硬件键盘记录器、软件键盘记录器以及木马等各种威胁下，密码面临巨大挑战。安全专家们通常会奉劝企业丢弃用户名/密码安全，转而采用多因素验证，因为现在多因素验证的价格逐渐下降，技术也更容易使用。现在让我们回过头来看看这些规则，看看是否有意义。 不要将密码写下来在我们公司，将密码写下来并没有被禁止。Nemertes研究公司的所有员工都是在家里办公，他们允许将密码写下来放入上锁的抽屉中以确保密码不会泄漏。通过将密码写下来，我们的用户可以使用更大更长的密码而不会忘记，并且也不再会用宠物的名字来当密码。将密码放入上锁的抽屉中，就可以通过物理安全来控制密码安全。选择长而复杂的密码. 如果你的机器上被安装了键盘记录器，其他密码保护措施都变得没有意义，不管你的密码是“ m7ruxM0Ipw7B ”还是“ Joe, Im running late for the meeting,

start without me! Andreas ”，键盘记录器都可以记录下来，这也使端点安全面临的最大威胁。随机密码很容易通过键盘记录来获取，甚至可能被自动检测(使用统计学或者字典过滤掉所有自然语言)。 不要将密码保存在浏览器这条规则是最害人的，如果最大的威胁是键盘记录器，那么最糟糕的事情就是继续输入相同的密码。如果你将密码保存在浏览器或者保存在密码保险箱中(有安全剪贴板功能)，这样就不会被键盘记录器记录。我为浏览器的密码保险箱使用的是非常复杂的住密码，然后将所有密码存在里面。 当你考虑所有的威胁问题时会发现，密码的“ 应用 ”安全性要比密码“ 绝对 ”安全性更加重要。我们应该需要遵守密码新规则以解决新的威胁和不断变化的密码窃取方式。 编辑特别推荐: 成本速度成关键解析 四种宽带接入技术 常用TCP端口作用及其操作建议