《防火墙》Firewall简介：哈里森-福特饰演一位国际银行保安主管，掌控银行的安全系统。犯罪份子绑架了他的家人，走投无路的福特，发誓要救回妻子和孩子……“防火墙”就是这场正邪大战的关键……   
  
　　名词解释：黑客的社会工程   
  
　　什么是社会工程？在安全领域，社会工程就是黑客们利用人与人之间的交往，取得被害人的信任，然后就是想干嘛干嘛了。社会工程是一种非技术手段的黑客行为，利用了网络安全体系中最没有办法控制、没有办法打补丁的一个因素——人。   
  
　　以下是正文：   
  
　　我这个人比较落伍，经常在电影热放很久以后才会去看，比如这次的firewall。   
  
　　因为是自己的本行，所以对这部电影有很高的兴趣，对整个过程也看的比较仔细。看完以后不仅慨叹，这是多么经典的一次暴力社会工程呀，只可惜精明的劫匪犯了一系列低级错误，造成最后的功亏一篑。真的应该好好总结一下这次的经验教训，以为后来者鉴。(叮咚!警察叔叔，找我有事吗?什么请我去喝茶?好呀好呀，我知道一个不错的茶馆。诶?去茶馆干嘛还带手铐呀?)   
  
　　嗯!嗯!嗯!郑重声明，以下评论仅做技术性讨论，并不代表本人支持任何类似的行为，或为其出谋划策。任何人利用本评论做任何事情都与本人无关。简而言之，我最多就是一个磨菜刀的(连卖菜刀的都不算)，持菜刀抢劫的行为与本人无关。   
  
　　ok，言归正传。首先来名词解释一下，什么是社会工程。在安全领域，社会工程就是黑客们利用人与人之间的交往，取得被害人的信任，然后就是想干嘛干嘛了。社会工程是一种非技术手段的黑客行为，利用了网络安全体系中最没有办法控制、没有办法打补丁的一个因素——人。这里介绍一个著名的针对Microsoft的社会工程案例，一个黑客给Microsoft的网管发了一封邮件，声称自己是Microsoft的员工，在欧洲出差，但是忘记的密码，大意的网管就发送了新的密码给这个人，黑客由此轻松的完成了入侵。这方面的详细信息，建议大家看美国著名黑客Kevin Mitnick的著作《The Art of Deception》，网上有下载，文笔很好，可以当小说看，还可以顺便练习一下E文。   
  
　　回到电影中来，《firewall》这部电影被我定义为典型的暴力社会工程案例，之所以这么说，是因为劫匪并没有依靠导演，尤其是国内导演，非常喜欢的有神迹的黑客完成抢劫(这是让所有的业内人士深恶痛绝的一种恶俗，随便乱敲一顿，然后对着“Bad command or files”就宣布入侵系统，靠，你当我们这些人都是狗屁呀。)，而是采用利用银行内部人员的方式完成抢劫，这显然属于社会工程的范畴。同时，显而易见，劫匪的社会工程属于非典型性的社会工程，因为他依靠的是暴力，而不是欺骗，这显然是Kevin Mitnick没有利用也没有介绍过的手段，估计真正社会工程黑客也不屑与用这种手段。用黎叔的话说:“最烦你们这帮打劫的，一点技术含量也没有。”   
  
　　这里面劫匪的领袖显然是一个很专业的劫匪，整个计划设计的很完善(并不完美，不完美的部分就是下面要讨论的)，盗取并模仿签名以及跟踪、监控、伪装等手段都非常的专业，估计这位兄弟有FBI或者CIA的背景。但是这位兄弟显然对信息技术的了解有限，所以这方面的工作更多的是依靠那位带着眼镜的文质彬彬的小伙，这小伙应该是一个写病毒和木马的高手。不过尽管劫匪都非常专业，团队的组合也是各有所长，几近完美。但是劫匪的整个计划却有若干重大的缺陷，下面就简单讨论一下。   
  
　　首先，劫匪们没有一个完整清晰的战略原则，这个原则就是——杀还是不杀，这是一个问题。劫匪们似乎想要杀死此次事件的所有被利用者，但是却莫名其妙的留下了人质，带着人质逃亡显然不是一个好主意，如果不想留尸体在家里，可以带着尸体上路。当然，好莱坞的导演可能为了一个大团员的结局不得不这样安排，但是我们这里讨论的是技术，而不是电影。那么究竟应该杀还是不杀呢?个人认为要么全杀要么不杀，而我比较倾向于不杀，因为寡人悟到了，最高的剑道是不杀，是和平。sorry，刺激太大，遗留至今。至于不杀的原因嘛，因为杀人太不优雅了，对于有追求有境界的劫匪来说，完全可以通过技术手段躲避警察的追踪，甚至可以让对方完全不发觉不报警。这在下面还有讨论。   
  
　　其次，劫匪的计划尽管完善，但是却有画蛇添足之感，比如逼迫女主人打电话假装婚外情，伪造情杀。这对于了解这对夫妇的人来说，显然很难让人相信。并且杀死那个人也很没有必要。劫匪完全可以找一个人来和那个人周旋(劫匪的人力资源很充足)，这个人只负责套取情报，并不直接参与事件的其他部分，没有人会将投资计划与抢劫计划联系在一起，这样也可以留下更少的线索。越简单的计划就越容易成功，当有更简单的方法的时候，为什么还要采用那么复杂的方法呢?    
  
  
　　再次，劫匪犯了一个非常低级的错误，就是在资金到位以后没有立刻更改那五个帐户的密码，正是这个疏忽造成了最后的功败垂成。如果抢劫成功后立刻更改密码，那么主人公的反击手段就不会成功。当然劫匪安排了干掉主人公的计划，但是任何行动都有成功与失败两种可能，所谓小心使得万年船，改个密码不是什么难事，却可以保证万无一失。况且我是不支持杀人的。   
  
　　最后讨论一下劫匪的一个非常好的方法，就是调出资金额度最高的一万个帐户，从每个帐户划取1万美元。这么做其实是降低案发的可能性的手段。这是因为一般人，除非对数字特别敏感的人比如会计什么的，一般只会关注数字的头两位，能够记住的也只是头两位，最多到第三位。比如现在我的帐户的头两位就是16，后面的就记不住了。那么如此大银行的前一万名大户应该都在千万百万的级别，少个1万什么的很难被发现，即使发现了也不会太在乎。比如我的帐户的第四位如果少了1，我也很难发现，即使发现了也绝对不会报案，你问我为什么?废话帐户少一毛钱就报案，你不怕警察告你妨碍公务呀，在说了，跨行查询还要3毛呢，谁知道这一毛钱是被黑客黑了还是被银行黑了。因为降低了案发的可能性，杀人的必要就更加不大了。   
  
　　需要注意的是，现在很多钓鱼的骇客们其实用的就是这种方法，钓鱼者们成功得到被害人的帐号及密码，取得了自由划拨资金的权限的时候，一般不会划走大量的资金，往往只是划走几十块钱就收手。你也许会认为这么点钱有点得不偿失，其实一个用户几十块，一万个用户就是就是几十万，十万个用户就是几百万，所谓积少成多集腋成裘是也。每个帐户由于损失很小，受害人常常不会发现，即使发现一般也不会报案，即使报案警察也不会重视，即使最终案发由于案值小也不会受到很严重的刑罚，甚至不会判刑，教育两句关几天就算了。所以作贼一定要做毛贼而不要做大盗，**树大招风，做大盗虽然风光，但是下场嘛**……   
  
　　ok，现在总结一下，这个劫案其实可以更加完美。改进的方案是，由单独的人充当投资方出面和主人公的朋友接触套取情报，甚至真的可以注册一个这样的公司，完事以后继续经营。然后一拨兄弟出面绑架跟踪干脏活，但注意对人质要和气，向对待客户一样对待他们，毕竟要靠他们才有钱赚嘛，做人要讲道理，做匪更要讲道理，要做匪先做人呀。资金到位后立刻更改帐户密码，然后释放人质从人间蒸发，地点推荐南美，那里银行提出来的款直接就干净了，没有记录的。况且最近巴西的事情大家都知道吧，能让警察惶惶不可终日的国家是什么样的境界呀，简直是匪的天堂。如果匪一并有了仁慈之心的话，临走之前可以与主人公神谈一次，分析一下案发的可能性和案发后主人公有嘴说不清的现实，再分几百万美元给主人公以示感谢和收买。当然不排除正义感极强的人还是会报案，但是绝大多数情况下，在有口难辩和有利可图之间，你会选择什么?这样一来，有了钱又不伤人，这是什么样的境界呀!这才是新一代有理想有道德有文化有知识有仁慈之心的匪呀!   
  
　　讨论完了劫匪，再来讨论一下银行，也省得警察叔叔认为我在这鼓励抢银行。这家银行在管理上显然存在一定的问题，最大的问题就是分权不够。在理论上，管理权和操作权是不能同时具有的，也就是说网络管理员是不可以拥有系统操作员的权限的，这应该是依靠严格的技术和管理保障的。这家银行显然没有做到这一点，从主人公几次轻易的转帐操作上就可以看出来。当然在现实中处于调试的方便，网管人员一般都会建立一个测试用的具有操作员权限的系统用户，一旦系统出现问题或者调试的时候就用这个用户做些操作来进行故障重现或者测试系统是否恢复正常。但是系统在设计的时候应该有足够的技术保障测试帐号不能操作正常帐户，并留下充分的审计记录。片中的银行显然没有做到这一点。此外银行内部员工之间缺乏强有力的相互制约机制，对主人公的充分信任，使得主人公可以轻易的做任何想做的操作，包括在监控台上自行操作的权利，从而删除了监控录像。诸如此类的管理问题，在这家银行里面应该是非常常见的，其实在现实的银行中也是非常常见的，但是确实是一个非常严重的安全隐患。