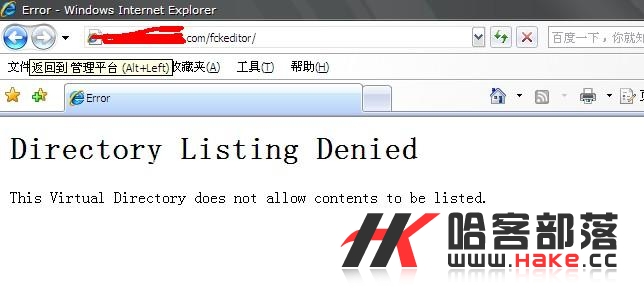
这个是我朋友的学校，我闲来无事，就检测下吧。看了下主站，竟然是asp的，赶快拿出工具射了一番，无果。后台也没找到，编辑器之类的更是没有了。我旁注了下，主站是独服，但是大家知道，大学的各个网站都是一个局域网，c段后会得到一些有用的信息。很快找到一个共青团分站。默认后台尝试，出现视频上传。找了半天也没找到路径，大马应该传了。



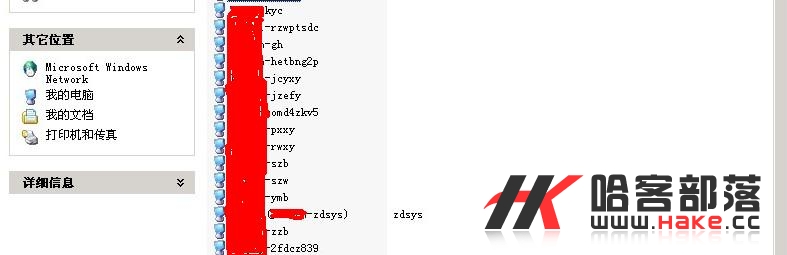
找到默认后台，尝试了几个弱口令都不对，aspx一般很喜欢用fckeditor，尝试，证明是有的。



至于fckeditor的漏洞，大家都比我了解，这里不细说，就是突破建立.asp文件夹，上传图片拿下这个分站。拿下后看了下，原来视频传到了一个video的文件夹，刚如果再想想，可能路径就找出来了。



大学的站权限基本都是很宽松的，提权成功。然后连接，服务器超过最大连接数，fuck！没关系，执行了鸽子，上线很快，query user logoff 这个站最终拿下，但是没用，我打开网上邻居看到不少站，但是没有主站，我为什么这么说呢，大家看图，我分析。



我入侵的那个服务器名字叫tw也就是团委，其他站后缀都是自己的网站名，但是主站的域名没有，我分别ping了所有服务器，这些站都是虚拟机，用了nat转换了ip地址，都是172的私网，同一网段。所以在局域网就可以浏览，没找到主站。继续入侵另一台用的依旧是fckeditor。拿下后找到主站。中间涂红的那个横杠就是主站的域名，他们用域名做了服务器的名称。Ping后找到主站地址。上了cain探嗅主站，一周断断续续过去了，没有有用信息，其他服务器依次拿下，主站依旧遥远。





转了一圈，又回到主站，既然是asp肯定好突破的多，继续换字典，扫后台，这次找到了一个很简陋的后台。



当然万能是肯定不行的，那么我尝试了下注入，过滤了get和post，那会不会没有过滤cookie

试试吧。果然没有过滤cookie，而且是mssql的数据库，利用pangoli直接写一句话进去。大家也可以用樱花浪子备份一句话，思路看自己。主站shell拿下。立即上pr程序卡死。连set一下也会卡死。我只能在shell里面继续翻看，找到了搜狗，想到以前看的一文章，替换

imeutil.exe 和 popup.dll，等待搜狗升级，添加用户sunwear。继续等待，过了差不多2周时间，sunwear出现。自此主站沦陷



由于是大概一个月前拿到的，虚拟机256m内存，就没多管，管理貌似做了限制，主要是方法，这个虚拟机pr之类的都卡死，解决交互，可以去组策略，前提pr能执行你的鸽子。也可以加入remote desktop users，（同样需要pr之类的能执行）方法多多。最后回顾一下，如果一开始就扫到那个后台，如果一开始就想到cookie，那么不需要这么长时间，拿站无非是细心加耐心以及用心。此文章只做技术交流，请各位大牛勿笑，小弟拜谢。

