有防火墙的网站整个入侵过程 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022__E6_9C_89_E9_98_B2_E7_81_AB_E5_c98_460944.htm 一、踩点 ping www.111.com 发现超时，可以是有防火墙或做了策略。再用superscan扫一下，发现开放的端口有很多个，初步估计是软件防火墙。 二、注入 从源文件里搜索关键字asp，找到了一个注入点。用nbsi注入，发现是sa口令登陆，去加了一个用户，显示命令完成。哈哈，看来管理员太粗心了。先上传一个webshell，上传了一个老兵的asp木马。接下来的就是个人习惯了，我平时入侵的习惯是先上传webshell，然后再把webshell提升为system权限。因为这样说可以说在入侵之时会非常的方便，我个人觉得这个方法非常好。 三、提升权限 先看哪些特权的： cs cript C:\Inetpub\AdminS cripts\adsutil.vbs get /W3SVC/InProcessIsapiApps 得到： Microsoft (R) Windows 脚本宿主版本 5.1 for Windows 版权所有(C) Microsoft Corporation 1996-1999. All rights reserved. InProcessIsapiApps : (LIST) (5 Items) "C:\WINNT\system32\idq.dll" "C:\WINNT\system32\inetsrv\httpext.dll" "C:\WINNT\system32\inetsrv\httpodbc.dll" "C:\WINNT\system32\inetsrv\ssinc.dll" "C:\WINNT\system32\msw3prt.dll" 把asp.dll加进去： cs cript C:\Inetpub\AdminS cripts\adsutil.vbs set /W3SVC/InProcessIsapiApps "C:\WINNT\system32\idq.dll" "C:\WINNT\system32 \inetsrv\httpext.dll" "C:\WINNT\system32\inetsrv\httpodbc.dll" "C:\WINNT\system32

\inetsrv\ssinc.dll"
"C:\WINNT\system32\msw3prt.dll""c:\winnt\system32
\inetsrv\asp.dll" 然后用asp木马加个用户，显示命令完成。 四、TerminalService 接下来就是开3389了，用net start显示，发现已开了TS服务，但端口上没有3389，觉得可能是改端口了。但事实上它们欺骗我的感情，我用netstat -an察看了一下，发现有3389，再从net start 里发现是对方的防火墙搞的鬼。算了，上传个木马吧，上传了一个改了特征码的20CN反弹木马，然后用木马在GUI下关掉了防火墙，再用3389登陆器登了上去，这里我这样做是因为我知道管理员一定不会在旁边。而对于这个时候，比较老道的方法大家可以用fpipe实现端口重定向，或者用httptunnel。和黑防里面说的那样，不过我试过没有成功过一次，而且我在收集资料里看到黑防的那篇和另外一个高手写的一模一样，不知道谁抄谁。还有一种工具是despoxy，(TCP tunnel for HTTP Proxies)大家有兴趣的话可以去试一下，它可以穿透http代理。 五、简单后门 1.改了FSO名，这样是让我自己享受，这个有system权限的马儿。 2.放了几个rootkit和几个网络上少见的后台。 3.我个从是不喜欢多放后台，觉得很烦。 六、Sniffer 1.TS界面下，下载了些嗅探器。先ARPsniffer图形的看了一下，晕死，没有一台内网机子。又看了一个外网，晕死,整个IP段都是。看来我的运行不错嘛，打开webdavscan查了一下，只有两三个IP是网站，而且是很小型的，接下来就没有什么动力了。 