后门程序Webshell

1.1概念

webshell就是以asp、php、jsp等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将asp或php后门文件与网站服务器WEB目录下正常的网页文件混在一起，然后就可以使用浏览器来访问asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的。如果确认webshell存在，这时我们需要做的就是首先联系网站负责人删除该木马。

常见的webshell后缀asp、cer、asa、cdx、aspx、ashx、php、jsp、jspx。

Webshell分类：小马（用于执行单一命令或是实现某种功能），大马（比小马功能更多）

一句话木马（需要webshell连接工具，常见的：蚁剑、CKnife、冰蝎、哥斯拉）

1.2方式

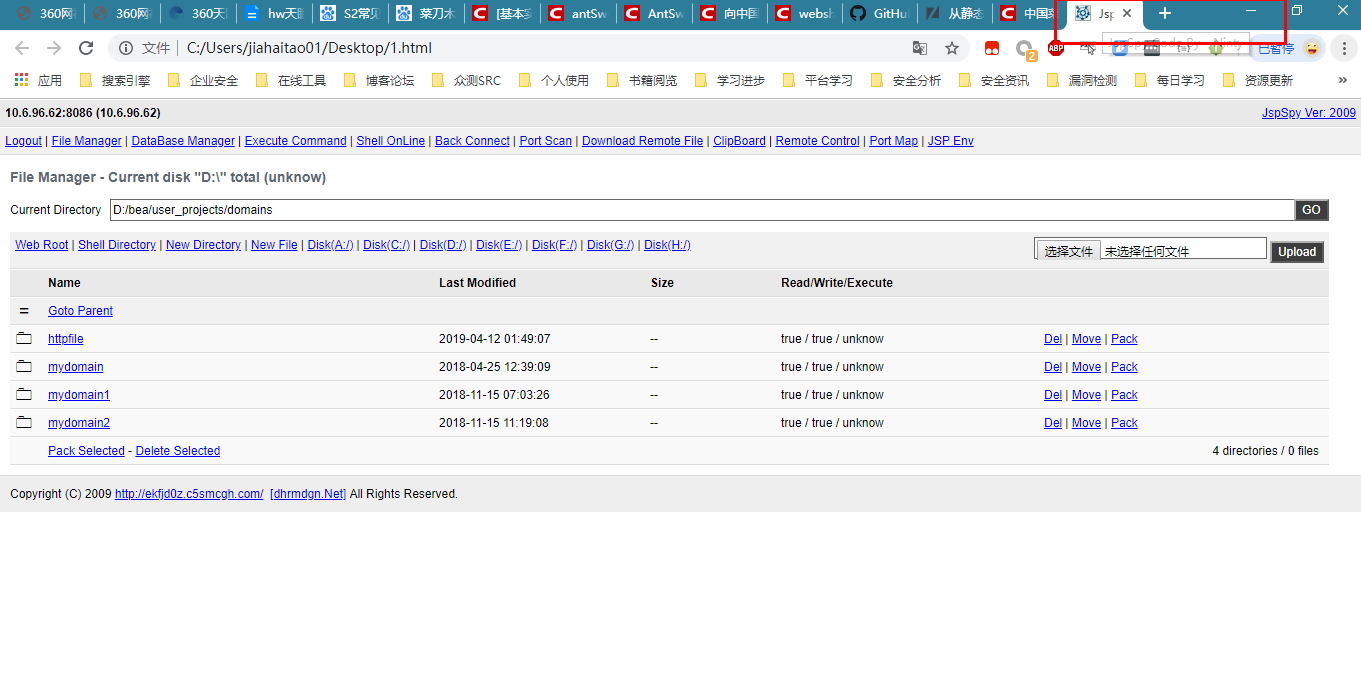
直接访问或是使用webshell管理工具。

1.3实战分析

小马通常是在url或是data里直接传参



大马通常需要登录，功能更多,，例如jspspy,aspspy等，需要使用密码登录，传输数据在data里面。



一句话木马 在告警中拼接host和URI得到webshell地址，访问，响应码200或是500(冰蝎)则说明webshell存在。

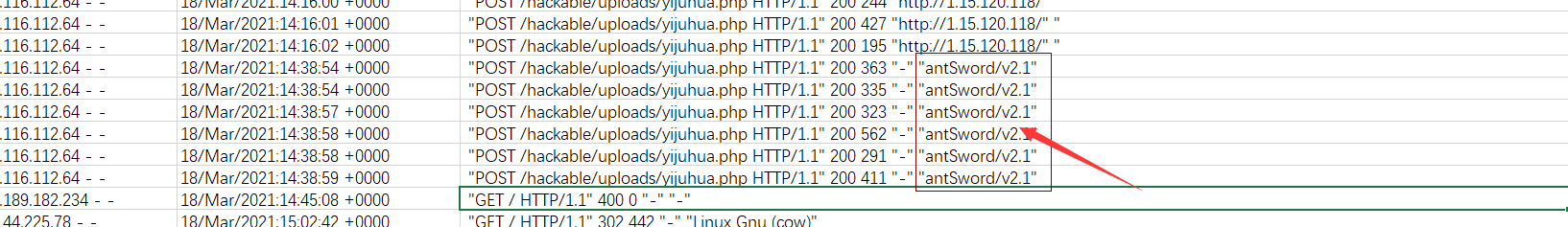
1.3.1利用跨平台版中国菜刀Cknife连接后门



1.3.2利用冰蝎Webshell工具连接后门



1.3.3利用冰蝎Webshell工具连接后门



1.3.1 马

大马

小马

一句话木马

1.3.1 防御检测