**八、安全事件处置**

公司网络因为受到攻击导致WEB应用服务器失陷，并在其中植入了恶意的Webshell，你作为网络的安全管理人员，需要排查并清除这些恶意的代码。

1. 使用D盾对C:\webapps中的文件进行扫描分析，对Webshell的名称截图并标注，并命名为P8-1.jpg。

**操作方法：打开D盾—查杀—选择目录—扫描C:\webapps—找到connect.php**

1. 确认Webshell之后，对Webshell文件创建的时间截图并标注，命名为P8-2.jpg。

**操作方法：打开D盾—查杀—选择目录—扫描C:\webapps—找到connect.php—右键“打开相关目录”—右键connect.php选择“属性”**

1. 分析Webshell内容，对Webshell的连接密码截图并标注，命名为P8-3.jpg。

**操作方法：打开D盾—查杀—选择目录—扫描C:\webapps—找到connect.php—右键“查看文件”**