专注APT攻击与防御
https://micropoor.blogspot.com/

reDuh简介：

reDuh是sensepost由2008-07年发布，从本质上讲，可以将JSP/PHP/ASP/ASPX等页面上传到目标服务器，便可以访问该服务器后面的主机。

BlackHat USA 2008介绍：
https://drive.google.com/open?id=1AqmtuBnHQJS-FjVHzJMNNWokda048By-

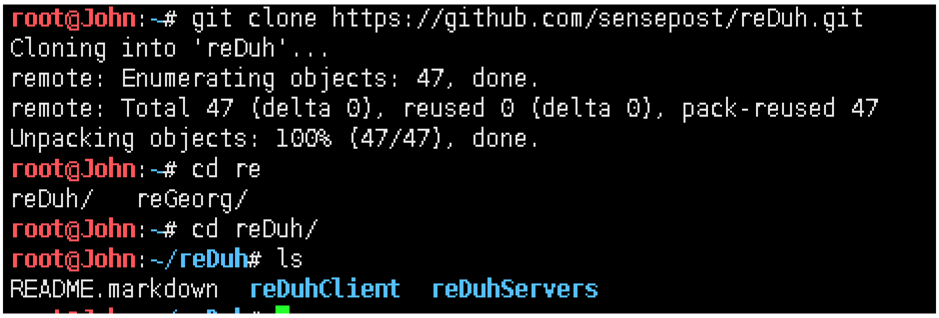
Github：
https://github.com/sensepost/reDuh

攻击机： 192.168.1.5　　　Debian
　　　192.168.1.4　　　Windows 7

靶机： 192.168.1.119　　Windows 2003

安装：

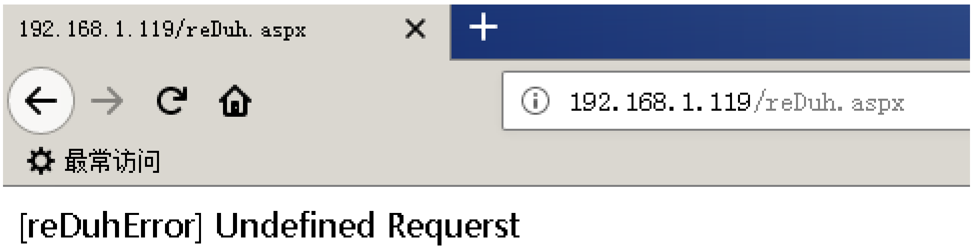
```
root@John:~# git clone https://github.com/sensepost/reDuh.git
Cloning into 'reDuh'...
remote: Enumerating objects: 47, done.
remote: Total 47 (delta 0), reused 0 (delta 0), pack-reused 47
Unpacking objects: 100% (47/47), done.
root@John:~# cd reDuh/
root@John:~/reDuh# ls
README.markdown reDuhClient reDuhServers
```



```
root@John:~# git clone https://github.com/sensepost/reDuh.git
Cloning into 'reDuh'...
remote: Enumerating objects: 47, done.
remote: Total 47 (delta 0), reused 0 (delta 0), pack-reused 47
Unpacking objects: 100% (47/47), done.
root@John:~# cd re
reDuh/    reGeorg/
root@John:~# cd reDuh/
root@John:~/reDuh# ls
README.markdown  reDuhClient  reDuhServers
```

靶机执行：

以aspx为demo。

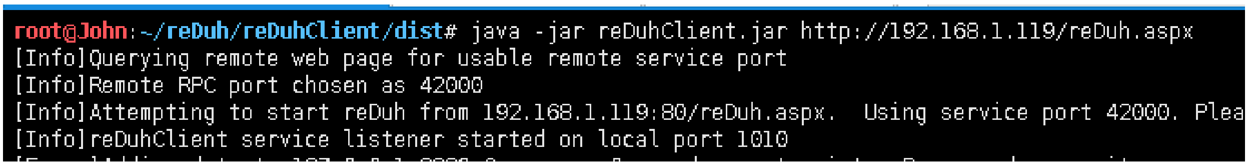


[reDuhError] Undefined Requerst

攻击机执行：

绑定端口：

```
root@John:~/reDuh/reDuhClient/dist# java -jar reDuhClient.jar http://192.168.1.119/reDuh.aspx
[Info]Querying remote web page for usable remote service port
[Info]Remote RPC port chosen as 42000
[Info]Attempting to start reDuh from 192.168.1.119:80/reDuh.aspx. Using service port 42000. Please wait...
[Info]reDuhClient service listener started on local port 1010
```



```
root@John:~/reDuh/reDuhClient/dist# java -jar reDuhClient.jar http://192.168.1.119/reDuh.aspx
[Info]Querying remote web page for usable remote service port
[Info]Remote RPC port chosen as 42000
[Info]Attempting to start reDuh from 192.168.1.119:80/reDuh.aspx.  Using service port 42000. Plea
[Info]reDuhClient service listener started on local port 1010
```

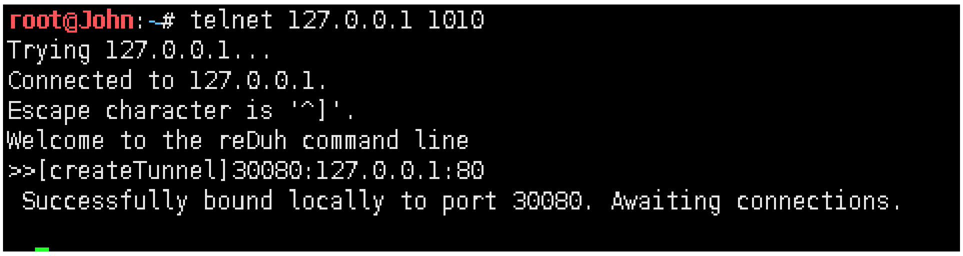
开启新terminal，建立隧道

命令如下：

[createTunnel][本地绑定端口]:127.0.0.1:[远程端口]

```
root@John:~# telnet 127.0.0.1 1010
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
```

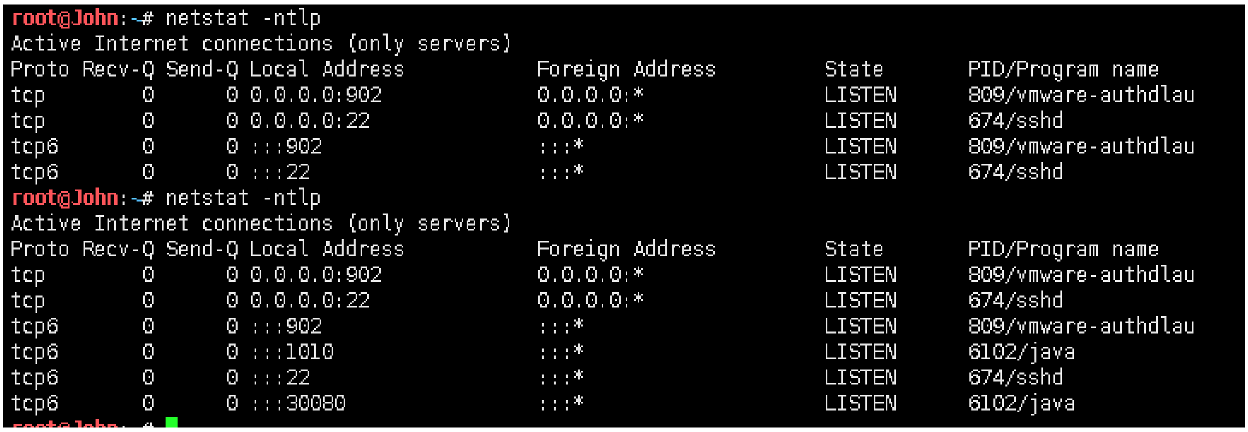
```
Welcome to the reDuh command line
>>[createTunnel]30080:127.0.0.1:80
 Successfully bound locally to port 30080. Awaiting connections.
```



```
root@John:~# telnet 127.0.0.1 1010
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Welcome to the reDuh command line
>>[createTunnel]30080:127.0.0.1:80
 Successfully bound locally to port 30080. Awaiting connections.
```

攻击机端口前后对比：

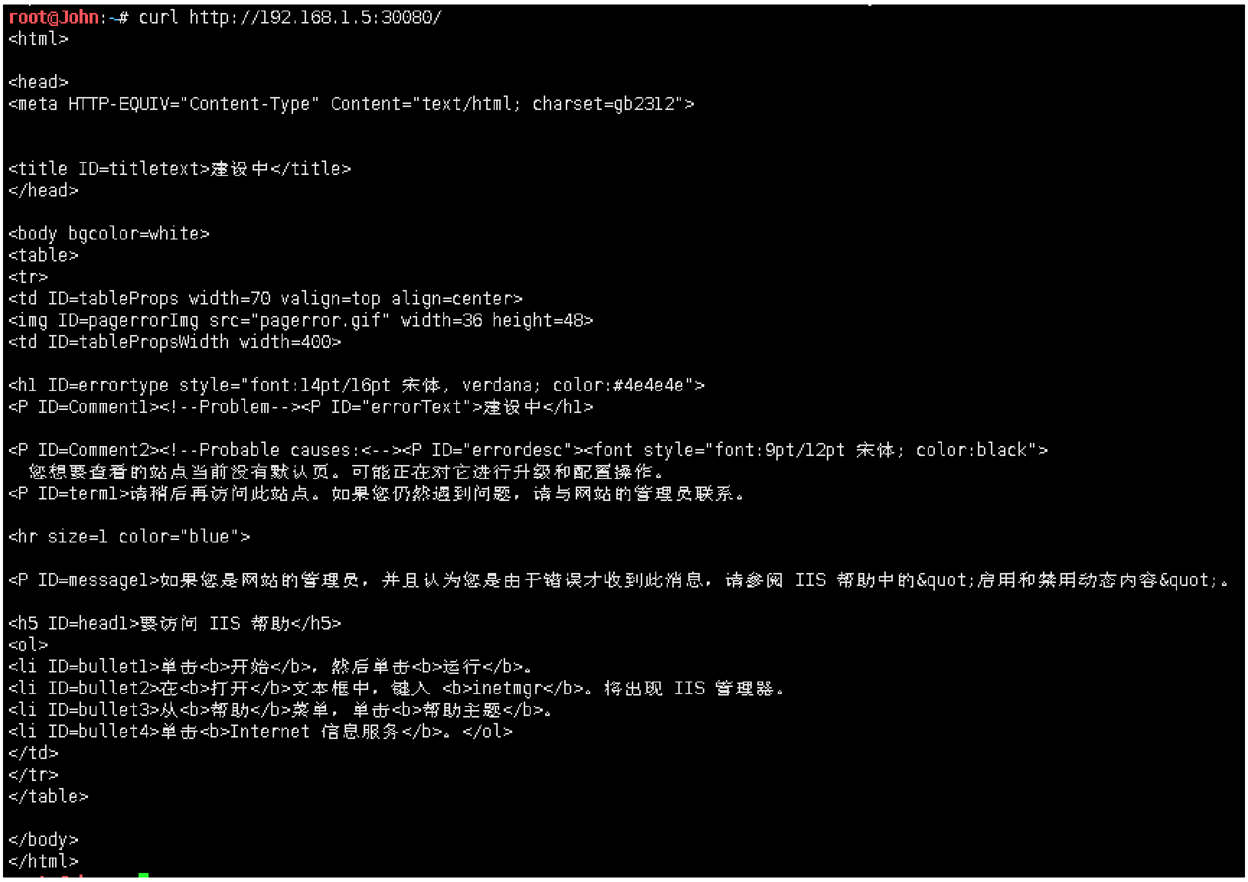
```
root@John:~# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:902 0.0.0.0:* LISTEN 809/vmware-authdlau
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 674/sshd
tcp6 0 0 :::902 :::* LISTEN 809/vmware-authdlau
tcp6 0 0 :::22 :::* LISTEN 674/sshd
root@John:~# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:902 0.0.0.0:* LISTEN 809/vmware-authdlau
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 674/sshd
tcp6 0 0 :::902 :::* LISTEN 809/vmware-authdlau
tcp6 0 0 :::1010 :::* LISTEN 6102/java
tcp6 0 0 :::22 :::* LISTEN 674/sshd
tcp6 0 0 :::30080 :::* LISTEN 6102/java

```



```
root@John:~# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:902             0.0.0.0:*               LISTEN      809/vmware-authdlau
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      674/sshd
tcp6       0      0 :::902                  :::*                    LISTEN      809/vmware-authdlau
tcp6       0      0 :::22                   :::*                    LISTEN      674/sshd
root@John:~# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:902             0.0.0.0:*               LISTEN      809/vmware-authdlau
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      674/sshd
tcp6       0      0 :::902                  :::*                    LISTEN      809/vmware-authdlau
tcp6       0      0 :::1010                 :::*                    LISTEN      6102/java
tcp6       0      0 :::22                   :::*                    LISTEN      674/sshd
tcp6       0      0 :::30080                :::*                    LISTEN      6102/java
root@John:~#
```

访问攻击机30080端口，既等价于访问靶机80端口

```
root@John:~# curl http://192.168.1.5:30080/
<html>

<head>
<meta HTTP-EQUIV="Content-Type" Content="text/html; charset=gb2312">


<title ID=titletext>建设中</title>
</head>

 <body bgcolor=white>

 ...

 </body>
 </html>
```



```
root@John:~# curl http://192.168.1.5:30080/
<html>

<head>
<meta HTTP-EQUIV="Content-Type" Content="text/html; charset=gb2312">


<title ID=titletext>建设中</title>
</head>

<body bgcolor=white>
<table>
<tr>
<td ID=tableProps width=70 valign=top align=center>
<img ID=pagerrorImg src="pagerror.gif" width=36 height=48>
<td ID=tablePropsWidth width=400>

<h1 ID=errortype style="font:14pt/16pt 宋体, verdana; color:#4e4e4e">
<P ID=Comment1><!--Problem--><P ID="errorText">建设中</h1>

<P ID=Comment2><!--Probable causes:<--><P ID="errordesc"><font style="font:9pt/12pt 宋体; color:black">
  您想要查看的站点当前没有默认页。可能正在对它进行升级和配置操作。
<P ID=term1>请稍后再访问此站点。如果您仍然遇到问题，请与网站的管理员联系。

<hr size=1 color="blue">

<P ID=message1>如果您是网站的管理员，并且认为您是由于错误才收到此消息，请参阅 IIS 帮助中的&quot;启用和禁用动态内容&quot;。

<h5 ID=head1>要访问 IIS 帮助</h5>
<ol>
<li ID=bullet1>单击<b>开始</b>，然后单击<b>运行</b>。
<li ID=bullet2>在<b>打开</b>文本框中，键入 <b>inetmgr</b>。将出现 IIS 管理器。
<li ID=bullet3>从<b>帮助</b>菜单，单击<b>帮助主题</b>。
<li ID=bullet4>单击<b>Internet 信息服务</b>。</ol>
</td>
</tr>
</table>

</body>
</html>
```

遗憾的是reDuh年代久远，使用繁琐，并官方已停止维护。但是它奠定了HTTP隧道。

- Micropoor