专注APT攻击与防御

https://micropoor.blogspot.com/

msf在非session 模式下与session模式下都支持第三方的加载与第三方框架的融合。代表参数为load。两种模式下的load 意义不同。本季主要针对非session模式下的load sqlmap情景。

加载Sqlmap后，主要参数如下：

1 Sqlmap Commands

2 =============== 3

4 Command Description

5 ‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

6 sqlmap\_connect sqlmap\_connect <host> [<port>]

7 sqlmap\_get\_data Get the resulting data of the task

8 sqlmap\_get\_log Get the running log of a task

9 sqlmap\_get\_option Get an option for a task

10 sqlmap\_get\_status Get the status of a task

11 sqlmap\_list\_tasks List the knows tasks. New tasks are not stored in D B, so lives as long as the console does

12 sqlmap\_new\_task Create a new task

13 sqlmap\_save\_data Save the resulting data as web\_vulns

14 sqlmap\_set\_option Set an option for a task

15 sqlmap\_start\_task Start the task

1 msf exploit(multi/handler) > help sqlmap

help 加载的模块名，为显示第三方的帮助文档。

msf上的sqlmap插件依赖于sqlmap的sqlmapapi.py 在使用前需要启动sqlmapapi.py

然后在msf上建立任务。

而sqlmap对msf也完美支持。

靶机：192.168.1.115，Sql server 2005 +aspx.net

构造注入点，如图1：

图1：

数据结构，如图2：

关于msf与sqlmap的结合在未来的系列中还会继续讲述，本季作为基础。

附录：

注入点代码：

1 <%@ Page Language="C#" AutoEventWireup="true" %>

2 <%@ Import Namespace="System.Data" %>

3 <%@ Import namespace="System.Data.SqlClient" %>

4 <!DOCTYPE html>

5 <script runat="server">

6 private DataSet resSet=new DataSet();

7 protected void Page\_Load(object sender, EventArgs e)

8 {

9 String strconn = "server=.;database=xxrenshi;uid=sa;pwd=123456";

10 string id = Request.Params["id"];

11 //string sql = string.Format("select \* from admin where id={0}", id);

12 string sql = "select \* from sys\_user where id=" + id;

13 SqlConnection connection=new SqlConnection(strconn);

14 connection.Open();

15 SqlDataAdapter dataAdapter = new SqlDataAdapter(sql, connection);

16 dataAdapter.Fill(resSet);

17 DgData.DataSource = resSet.Tables[0];

18 DgData.DataBind();

19 Response.Write("sql:<br>"+sql);

20 Response.Write("<br>Result:");

21 } 22

23 </script> 24

25 <html xmlns="http://www.w3.org/1999/xhtml">

26 <head runat="server">

27 <meta http‐equiv="Content‐Type" content="text/html; charset=utf‐8"/>

28 <title></title>

29 </head>

30 <body>

31 <form id="form1" runat="server">

32 <div> 33

34 <asp:DataGrid ID="DgData" runat="server" BackColor="White" BorderColo r="#3366CC"

35 BorderStyle="None" BorderWidth="1px" CellPadding="4"

36 HeaderStyle‐CssClass="head" Width="203px">

37 <FooterStyle BackColor="#99CCCC" ForeColor="#003399" />

38 <SelectedItemStyle BackColor="#009999" Font‐Bold="True" ForeColor="#C CFF99" />

39 <PagerStyle BackColor="#99CCCC" ForeColor="#003399" HorizontalAlign="Left"

40 Mode="NumericPages" />

41 <ItemStyle BackColor="White" ForeColor="#003399" />

42 <HeaderStyle CssClass="head" BackColor="#003399" Font‐Bold="True" Fore Color="#CCCCFF"></HeaderStyle>

43 </asp:DataGrid> 44

45 </div>

46 </form>

47 </body>

48 </html>

Micropoor