【译】Metasploit：漏洞利用程序评级

王一航 / 2018-06-13 14:13:39 / 浏览数 5435 新手 入门资料 顶(0) 踩(0)

- 原文地址：https://github.com/rapid7/metasploit-framework/wiki/Exploit-Ranking
- 作者：Metasploit Community
- 译者：王一航 2018-06-13
- 校对：王一航 2018-06-13

每一个漏洞利用模块基于它们的对目标系统的潜在影响都被标记了一个 Rank 字段。
用户可以基于 Rank 对漏洞利用模块进行搜索，分类以及排序。

模块评级的实现方式是在模块的顶级类（译者注：Ruby 语言的特性，一个 .rb 文件可以是一个 Module 或者一个 Class）中添加一个 Rank 常量

```
class MetasploitModule < Msf::Exploit
   Rank = LowRanking
   def initialize(info={})
       ...
   end
   ...
end
```

Rank 常量的值可以是下面的表格中的其中之一，按照可靠性降序排列。

Ranking	Description
ExcellentRanking	漏洞利用程序绝对不会使目标服务崩溃，就像 SQL 注入，命令执行，远程文件包含，本地文件包含等等。除非有特殊情况，典型的内存破坏利 Escape() ）
GreatRanking	该漏洞利用程序有一个默认的目标系统，并且可以自动检测适当的目标系统，或者在目标服 Shell 退出后的返回地址，否则当 Shell 结束后，目标服务器会崩溃掉。 ）
GoodRanking	The exploit has a default target and it is the "common case" for this type of software (English, Windows 7 for a desktop app, 2012 for server, etc). 该漏洞利用程序有一个默认目标系统，并且是这种类型软件的“常见情况”（英文，桌面应用 7，服务器的2012等）（译者注：这段翻译的不是很懂，因此保留原文）
NormalRanking	该漏洞利用程序是可靠的，但是依赖于特定的版本，并且不能或者不能可靠地自动检测。
AverageRanking	该漏洞利用程序不可靠或者难以利用。
LowRanking	对于通用的平台而言，该漏洞利用程序几乎不能利用（或者低于 50% 的利用成功率）
ManualRanking	该漏洞利用程序不稳定或者难以利用并且基于拒绝服务（DOS）。如果一个模块只有在用户

Rank 的值在模块类对象或者类实例中被设置

```
modcls = framework.exploits["windows/browser/ie_createobject"]
modcls.rank      # => 600
modcls.rank_to_s # => "excellent"

mod = modcls.new
mod.rank      # => 600
mod.rank_to_s # => "excellent"
```


上一篇：【译】Metasploit：Met... 下一篇：一次红队之旅
1. 0 条回复
   - 动动手指，沙发就是你的了！

目录