登录

【原创】中间件漏洞检测(MiddlewareScan)

wolf / 2016-11-09 01:44:31 / 浏览数 6515 安全工具 工具 顶(0) 踩(0)

由python编写的轻量级中间件漏洞检测框架，实现针对中间件的自动化检测，端口探测->中间件识别->漏洞检测->获取webshell
参数说明：
-h
必须输入的参数，支持ip(192.168.1.1)，ip段（192.168.1），ip范围指定（192.168.1.1-192.168.1.254）,ip列表文件（ip.ini），最多限制一次可扫描65535个IP。
-p 指定要扫描端口列表，多个端口使用,隔开
例如：7001,8080,9999。未指定即使用内置默认端口进行扫描(80,4848,7001,7002,8000,8001,8080,8081,8888,9999,9043,9080)
-m 指定线程数量 默认100线程
-t 指定HTTP请求超时时间，默认为10秒，端口扫描超时为值的1/2。
默认漏洞结果保存在 result.log中
例子：
python F-MiddlewareScan.py -h 10.111.1
python F-MiddlewareScan.py -h 192.168.1.1
python F-MiddlewareScan.py -h 10.111.1.1-10.111.2.254 -p 80,7001,8080 -m 200 -t 6
效果图：

漏洞检测脚本以插件形式存在，内置了19个漏洞插件，可以自定义添加修改漏洞插件，存放于plugins目录，插件标准非常简单，只需对传入的IP，端口，超时进行操作，成
新增插件需要在 plugin_config.ini配置文件中新增关联（多个漏洞插件以逗号隔开）。
中间件识别在discern_config.ini文件中配置（支持文件内容和header识别）
开源项目地址：https://github.com/ywolf/F-MiddlewareScan
[i]此工具仅可用于授权的渗透与自身的检测中，请勿用于非法入侵。[/i]

点击收藏 | 1 关注 | 1

上一篇：PHP伪协议 下一篇：渗透Facebook的思路與發現

1. 8 条回复


master 2016-11-09 06:00:11

wolf的工具，都是经典。

0 回复Ta


ms0x0 2016-11-09 06:15:50

这个Good，赞。 可以批量了。。。。。

0 回复Ta


道 2016-11-09 08:00:38

人民的币+20.。。。。

0 回复Ta


hope 2016-11-09 11:03:34

以前在土司上下载了，很好用

0 回复Ta


mycookie 2017-08-24 01:03:49

以前在土司上下载了，很好用

0 回复Ta


only 2017-08-28 02:38:39

赞一个!!!!!

0 回复Ta


only 2017-08-28 02:39:22

为防止此脚本被恶意使用，此项目已删除。

0 回复Ta

飞将 2018-01-17 15:27:12

这个项目已经被删除，有木有大佬能够提供该资源

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