登录

【原创】网络资产信息扫描(F-NAScan)

wolf / 2016-11-08 08:25:41 / 浏览数 5312 安全工具 工具 顶(0) 踩(0)

网络资产信息扫描
  在渗透测试(特别是内网)中经常需要对目标进行网络资产收集，即对方服务器都有哪些IP，IP上开了哪些端口，端口上运行着哪些服务，此脚本即为实现此过程。
  相比其他探测脚本有以下优点：1、轻巧简洁,只需python环境，无需安装额外外库。2、扫描完成后生成独立页面报告。
  此脚本的大概流程为 ICMP存活探测–>端口开放探测–>端口指纹服务识别–>提取快照(若为WEB)–>生成结果报表
运行环境:python 2.6 +

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：22,23,80,3306。未指定即使用内置默认端口进行扫描(21,22,23,25,53,80,110,139,143,389,443,445,465,873,993,995,1080,1723,1433,1521,3306,3389,3690,5432
  -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。
  -n 不进行存活探测(ICMP)直接进行扫描。
  结果报告保存在当前目录(扫描IP-时间戳.html)。
例子：
  python NAScan.py -h 10.111.1
  python NAScan.py -h 192.168.1.1
  python NAScan.py -h 10.111.1.1-10.111.2.254 -p 80,7001,8080 -m 200 -t 6
  python NAScan.py -h ip.ini -p port.ini -n
  服务识别在server_info.ini文件中配置
  格式为：服务名|默认端口|正则 例 ftp|21|^220.*?ftp|^220-
  正则为空时则使用端口进行匹配，否则以正则匹配结果为准。

效果图

项目开源地址 https://github.com/ywolf/F-NAScan

上一篇：微软官方的DLL注入工具 下一篇：MySQL在渗透测试中的应用

1. 6 条回复


r4bb1t_ 2016-11-08 09:00:38

这个输出格式不错

0 回复Ta


笑然 2016-11-08 09:17:51

版主果然给力

0 回复Ta


master 2016-11-09 05:57:19

又见师傅的工具了。感谢分享

0 回复Ta


ms0x0 2016-11-09 06:15:20

工具代码写的挺好的，

如果是安全人员我感觉应该会挺喜欢的，
日过是渗透人员，我更希望是EXE的。
因为在内网的入口点，客户机上很少有PY 的。
（ PS，最好加上时间限制，我不追求速度，我追求的是不被防火墙拦截。。 ）

0 回复Ta


hades 2016-11-09 08:23:12

看来现在如果优雅的不被WAF发现是值得好好探索的一个问题

0 回复Ta

ms0x0 2016-11-21 03:29:48

对对对

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