Nmap速查手册

2014/12/17 11:24 | 我是壮丁 | 技术分享 | 占个座先 | 捐赠作者

From:http://highon.coffee/docs/nmap/

0x00:说明

只是一个快速查询手册,理论的东西都没有补充,欢迎大家积极在评论区补充自己常用的参数,O(∩_∩)O

0x01:nmap功能介绍

1. 主机存活检测
2. 端口探测
3. 服务识别
4. 操作系统识别
5. 硬件地址检测
6. 服务版本识别
7. 漏洞扫描,使用nmap自带脚本

0x02:简单示例

使用ping检测10.0.0.0/24这个网段

```
nmap -sP 10.0.0.0/24
```

使用SYN的方法对全端口进行扫描,在aggressive(4)的时间模板下,同时对开放的端口进行端口识别

```
nmap -p1-65535 -sV -sS -T4 target
```

PS: -T代表的是扫描的时候,一些控制选项(TCP的延迟时间,探测报文之间的间隔等)的集合,具体的man nmap一下就知道了

使用SYN扫描,在aggressive(4)的时间模板下,探测操作系统的类型和版本,还有显示traceroute的结果,结果输出较为详细

```
nmap -v -sS -A -T4 target
```

使用SYN扫描,在insane(5)的时间模板下,探测操作系统的类型和版本,还有显示traceroute的结果,结果输出较为详细

```
nmap -v -sS -A -T5 target
```

使用SYN扫描,在insane(5)的时间模板下,探测操作系统的类型,还有显示traceroute的结果,操作系统的类型,结果输出较为详细

```
nmap -v -sV -O -sS -T5 target
```

使用SYN的方法对全端口进行扫描,同时对开放的端口进行端口识别,在aggressive(4)的时间模板下,探测操作系统的类型还有显示traceroute的结果,结果输出较为详细

```
nmap -v -p 1-65535 -sV -O -sS -T4 target
```

用SYN的方法对全端口进行扫描,同时对开放的端口进行端口识别,在insane(5)的时间模板下,探测操作系统的类型,还有显示traceroute的结果,结果输出较为详细

```
nmap -v -p 1-65535 -sV -O -sS -T5 target
```

从文件中读取需要扫描的IP列表

```
nmap -iL ip-address.txt
```

Nmap输出格式

扫描的结果输出到屏幕,同时会存储一份到grep-output.txt

```
nmap -sV -p 139,445 -oG grep-output.txt 10.0.1.0/24
```

公告

召唤时事热点以及目前知识库略缺的内容。
议题召唤中的内容：

1. 最新的事件分析和安全预警
2. 乌云主站漏洞总结
3. 业内前沿最新技术

如果你觉得有更好的议题方向
可以直接 投稿 或者发邮件到
drops@wooyun.org

订阅更新

分类

- 漏洞分析 (139)
- 技术分享 (244)
- 工具收集 (27)
- 业界资讯 (27)
- 运维安全 (63)
- web安全 (118)
- 渗透案例 (5)
- 移动安全 (25)
- 无线安全 (6)
- 数据库安全 (3)
- 二进制安全 (29)

最新日志

- jother编码之谜
- 常见的HTTPS攻击方法
- Android Broadcast Security
- One git command may cause you hacked(CVE-2014-9390)
- CoolPad backdoor CoolReaper
- 某EXCEL漏洞样本shellcode分析
- Nmap速查手册
- IPS BYPASS姿势
- False SQL Injection and Advanced Blind SQL Injection
- Android Content Provider Security

最新评论

mramydnei 在 jother编码之谜
jother是天马行空发明的？？？

px1624 在 jother编码之谜
学习了！

DEVILK 在 APK签名校验绕过
不错的文章~ 但是并不能绕过selinux

test# 在 jother编码之谜
神奇的Javascript Brainfuck

扫描结果输出为html

```
nmap -sS -sV -T5 10.0.1.99 --webxml -oX - | xsltproc --output file.html
```

Nmap扫描Netbios

在子网中发现开放netbios的IP

```
nmap -sV -v -p139,445 10.0.0.1/24
```

扫描指定netbios的名称

```
nmap -sU --script nbstat.nse -p 137 target
```

扫描指定的目标,同时检测相关漏洞

```
nmap --script-args=unsafe=1 --script smb-check-vulns.nse -p 445 target
```

将nmap的80端口的扫描结果,通过管道交给nikto进行扫描

```
Nmap Nikto Scan nmap -p80 10.0.1.0/24 -oG - | nikto.pl -h -
```

将nmap的80,443端口的扫描结果,通过管道交给nikto进行扫描

```
nmap -p80,443 10.0.1.0/24 -oG - | nikto.pl -h -
```

0x03:Nmap参数详解

Nmap支持主机名,ip,网段的表示方式

例如:blah.highon.coffee, namp.org/24, 192.168.0.1;10.0.0-25.1-254

```
-iL filename                    从文件中读取待检测的目标,文件中的表示方法支持机名,ip,网段
-iR hostnum                     随机选取,进行扫描.如果-iR指定为0,则是无休止的扫描
--exclude host1[, host2]        从扫描任务中需要排除的主机
--exculdefile exclude_file      排除文件中的IP,格式和-iL指定扫描文件的格式相同
```

主机发现

```
-sL                     仅仅是显示,扫描的IP数目,不会进行任何扫描
-sn                     ping扫描,即主机发现
-Pn                     不检测主机存活
-PS/PA/PU/PY[portlist]  TCP SYN Ping/TCP ACK Ping/UDP Ping发现
-PE/PP/PM               使用ICMP echo, timestamp and netmask 请求包发现主机
-PO[prococol list]      使用IP协议包探测对方主机是否开启
-n/-R                   不对IP进行域名反向解析/为所有的IP都进行域名的反响解析
```

扫描技巧

```
-sS/sT/sA/sW/sM                 TCP SYN/TCP connect()/ACK/TCP窗口扫描/TCP Maimon扫描
-sU                             UDP扫描
-sN/sF/sX                       TCP Null, FIN, and Xmas扫描
--scanflags                     自定义TCP包中的flags
-sI zombie host[:probeport]     Idlescan
-sY/sZ                          SCTP INIT/COOKIE-ECHO 扫描
-sO                             使用IP protocol 扫描确定目标机支持的协议类型
-b "FTP relay host"             使用FTP bounce scan
```

指定端口和扫描顺序

```
-p                      特定的端口 -p80,443 或者 -p1-65535
-p U:PORT               扫描udp的某个端口, -p U:53
-F                      快速扫描模式,比默认的扫描端口还少
-r                      不随机扫描端口,默认是随机扫描的
--top-ports "number"    扫描开放概率最高的number个端口,出现的概率需要参考nmap-services文件,ubuntu中该文件位于/usr/share/nmap.nmap默认扫前1000个
--port-ratio "ratio"    扫描指定频率以上的端口
```

服务版本识别

```
-sV                             开放版本探测,可以直接使用-A同时打开操作系统探测和版本探测
--version-intensity "level"     设置版本扫描强度,强度水平说明了应该使用哪些探测报文。数值越高,服务越有可能被正确识别。默认是7
--version-light                 打开轻量级模式,为--version-intensity 2的别名
--version-all                   尝试所有探测,为--version-intensity 9的别名
--version-trace                 显示出详细的版本侦测过程信息
```

脚本扫描

```
-sC                             根据端口识别的服务,调用默认脚本
--script="Lua scripts"          调用的脚本名
--script-args=n1=v1,[n2=v2]     调用的脚本传递的参数
--script-args-file=filename     使用文本传递参数
--script-trace                  显示所有发送和接收到的数据
--script-updatedb               更新脚本的数据库
--script-help="Lua script"      显示指定脚本的帮助
```

OS识别

```
-O              启用操作系统检测,-A来同时启用操作系统检测和版本检测
--osscan-limit  针对指定的目标进行操作系统检测(至少需确知该主机分别有一个open和closed的端口)
--osscan-guess  推测操作系统检测结果,当Nmap无法确定所检测的操作系统时，会尽可能地提供最相近的匹配，Nmap默认进行这种匹配
```

防火墙/IDS躲避和哄骗

```
-f; --mtu value                 指定使用分片、指定数据包的MTU.
-D decoy1,decoy2,ME             使用诱饵隐蔽扫描
-S IP-ADDRESS                   源地址欺骗
-e interface                    使用指定的接口
-g/ --source-port PROTNUM       使用指定源端口
--proxies url1,[url2],...       使用HTTP或者SOCKS4的代理

--data-length NUM               填充随机数据让数据包长度达到NUM
--ip-options OPTIONS            使用指定的IP选项来发送数据包
--ttl VALUE                     设置IP time-to-live域
--spoof-mac ADDR/PREFIX/VEBDOR  MAC地址伪装
--badsum                        使用错误的checksum来发送数据包
```

Nmap 输出

```
-oN                 将标准输出直接写入指定的文件
-oX                 输出xml文件
-oS                 将所有的输出都改为大写
-oG                 输出便于通过bash或者perl处理的格式,非xml
-oA BASENAME        可将扫描结果以标准格式、XML格式和Grep格式一次性输出
-v                  提高输出信息的详细度
-d level            设置debug级别,最高是9
--reason            显示端口处于带确认状态的原因
--open              只输出端口状态为open的端口
--packet-trace      显示所有发送或者接收到的数据包
--iflist            显示路由信息和接口,便于调试
--log-errors        把日志等级为errors/warings的日志输出
--append-output     追加到指定的文件
--resume FILENAME   恢复已停止的扫描
--stylesheet PATH/URL   设置XSL样式表，转换XML输出
--webxml            从namp.org得到XML的样式
--no-sytlesheet     忽略XML声明的XSL样式表
```

其他nmap选项

```
-6                      开启IPv6
-A                      OS识别,版本探测,脚本扫描和traceroute
--datedir DIRNAME       说明用户Nmap数据文件位置
--send-eth / --send-ip  使用原以太网帧发送/在原IP层发送
--privileged            假定用户具有全部权限
--unprovoleged          假定用户不具有全部权限,创建原始套接字需要root权限
-V                      打印版本信息
-h                      输出帮助
```

0x04:例子

整个子网检测的Netbios

```
Nmap -sV -v -p 139,445 10.0.1.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-11 21:26 GMT
Nmap scan report for nas.decepticons 10.0.1.12
Host is up (0.014s latency).

PORT STATE SERVICE VERSION
139/tcp open netbios-ssn Samba smbd 3.X (workgroup: MEGATRON)
445/tcp open netbios-ssn Samba smbd 3.X (workgroup: MEGATRON)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 256 IP addresses (1 hosts up) scanned in 28.74 seconds
```

Nmap 查找Netbios名称

```
nmap -sU --script nbstat.nse -p 137 10.0.1.12
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-11 21:26 GMT
Nmap scan report for nas.decepticons 10.0.1.12
Host is up (0.014s latency).

PORT STATE SERVICE VERSION
137/udp open netbios-ns
```

```
Host script results:
|_nbstat: NetBIOS name: STARSCREAM, NetBIOS user: unknown, NetBIOS
MAC: unknown (unknown)
Nmap done: 256 IP addresses (1 hosts up) scanned in 28.74 seconds
```

如果开启Netbios服务,检查是否存在漏洞

```
nmap --script-args=unsafe=1 --script smb-check-vulns.nse -p
445 10.0.0.1

Nmap scan report for ie6winxp.decepticons (10.0.1.1)
Host is up (0.00026s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
Host script results:
| smb-check-vulns:
| MS08-067: VULNERABLE
| Conficker: Likely CLEAN
| regsvc DoS: NOT VULNERABLE
| SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
|_ MS07-029: NO SERVICE (the Dns Server RPC service is inactive)
Nmap done: 1 IP address (1 host up) scanned in 5.45 seconds
```

根据扫描结果,发现存在MS08-067漏洞

0x05参考

原文

http://highon.coffee/docs/nmap/

Namp官网的完整手册

https://svn.nmap.org/nmap/docs/nmap.usage.txt

Nmap官方的中文手册

http://nmap.org/man/zh/

国内的一篇讲Nmap的,写的挺不错的

http://blog.csdn.net/aspirationflow/article/details/7694274

终极必杀:

man nmap

相关日志
- MongoDB安全配置
- InsightScan:Python多线程Ping/端口扫描 + HTTP服务/APP 探测，可生成Hydra用的IP列表
- Tor隐身大法 —— 用Tor来帮助我们进行渗透测试
- 逆向基础（八）
- 逆向基础（十一）
- 一种自动化检测 Flash 中 XSS 方法的探讨

上一篇:IPS BYPASS姿势
下一篇:某EXCEL漏洞样本shellcode分析

回复该留言

Teachsec | 2014/12/17 15:29 | #

来点高级用法。

回复该留言

_Thorns | 2014/12/17 15:31 | #

支持下！~

回复该留言

草根 | 2014/12/17 16:22 | #

支持

回复该留言

泳少 | 2014/12/17 23:15 | #

收藏了

回复该留言

小涛 | 2014/12/18 19:01 | #

同胞 2 块钱收了你 嘿嘿嘿嘿i ~

回复该留言

Jumbo | 2014/12/19 23:48 | #

我还以为翻错页了

回复该留言

nmaps | 2014/12/22 16:22 | #

nmap 经久不衰阿

回复该留言

发表评论

您已经以 orange 的身份登录。 注销 »

验证码*

发表评论[Ctrl+Enter]