2.4-端口服务信息

无涯老师

上节课回顾

1、DNS服务器的类型
2、ping / nslookup
3、IP归属信息
4、如何获取CDN背后的真实IP

课程大纲

1、端口扫描思路和代码实现
2、常见端口及漏洞
3、端口扫描工具

01

端口扫描思路和代码实现

查看本机端口信息

Windows
netstat -aon|findstr 3306

Linux
netstat -an|grep 3306

远程机器端口

telnet 192.168.142.137 80

wget 192.168.142.137 80

nc -vz 192.168.142.137 445

python代码扫描

wscan.py

02 常见端口及漏洞

常见端口

https://nsrc.org/workshops/2009/summer/presentations/day3/common-ports.pdf

分类

1、文件共享服务
2、远程连接服务
3、Web应用服务
4、数据库服务
5、邮件服务
6、网络常见协议
7、其他服务端口

文件共享服务端口

端口号	端口说明	攻击方向
21/22/69	FTP/SFTP文件传输协议	允许匿名上传、下载、爆破和嗅探操作
2049	NFS服务（Network File System）	配置不当
139	Samba服务	爆破、未授权访问、远程代码和执行
389	LDAP目录访问协议	注入、允许匿名访问、弱口令

远程连接服务端口

端口号	端口说明	攻击方向
22	SSH远程连接	爆破、SSH隧道及内网代理转发、文件传输
23	Telnet远程连接	爆破、嗅探、弱口令
3389	RDP远程桌面连接	Shift后门（Windows Server2003以下的系统）、爆破
5900	VNC	弱口令爆破
5632	PcAnywhere远程控制服务	抓密码、代码执行

web应用服务端口

端口号	端口说明	攻击方向
80/443/8080	常见的web服务端口	Web攻击、爆破、对应服务器版本漏洞
7001/7002	Weblogic控制台	Java反序列化、弱口令
8080/8089	Jboss/resin/jetty/Jenkins	反序列化、控制台弱口令
9090	Websphere控制台	Java反序列化、弱口令
4848	Glassfish控制台	弱口令
1352	Lotus domino邮件服务	弱口令、信息泄露、爆破
10000	Webmin-web控制面板	弱口令

数据库服务端口

端口号	端口说明	攻击方向
3306	MySQL	注入、提权、爆破
1433	MSSQL数据库	注入、提权、SA弱口令
1521	Oracle数据库	TNS爆破、注入、反弹shell
5432	PostgreSQL数据库	爆破、注入、弱口令
27017/27018	MongoDB	爆破、未授权访问
6379	Redis数据库	可尝试未授权访问、弱口令爆破
5000	Sysbase/DB2数据库	爆破、注入

邮件服务端口

端口号	端口说明	攻击方向
25	SMTP邮件服务	邮件伪造
110	POP3协议	爆破、嗅探
143	IMAP协议	爆破

网络常见协议端口

端口号	端口说明	攻击方向
53	DNS域名系统	允许区域传送、DNS劫持、缓存投毒、欺骗
67/68	DHCP服务	劫持、欺骗
161	SNMP协议	爆破、搜集目标内网信息

特殊服务端口

端口号	端口说明	攻击方向
2181	Zookeeper服务	未授权访问
8069	Zabbix服务	远程执行、SQL注入
9200/9300	ElasticSearch服务	远程执行
11211	Memcached服务	未授权访问
512/513/514	Linux Rexec服务	爆破、rlogin登录
873	Rsync服务	匿名访问、文件上传
3690	SVN服务	SVN泄露、未授权访问
50000	SAP Management Console	远程执行

03 端口扫描工具

Nmap

Nmap（Network Mapper）
https://nmap.org/

1）扫描主机(Host Discovery)
2）扫描端口(Port Scanning)
3）探测操作系统、软件版本 (Operating System Detection、Version Detection)

参数类型

nmap --help

- TARGET SPECIFICATION:目标，对什么进行扫描，比如是域名、IP或者网络
- HOST DISCOVERY:主机发现，怎么对主机进行扫描，比如简单扫描，还是全部扫一遍，或者用相应的协议扫
- SCAN TECHNIQUES:扫描技术，协议的设置
- PORT SPECIFICATION AND SCAN ORDER:端口和扫描顺序设置
- SERVICE/VERSION DETECTION:服务和版本识别
- SCRIPT SCAN:使用脚本，nmap本身内置了大量的lua脚本，而且还可以自己编写脚本
- OS DETECTION:操作系统识别
- TIMING AND PERFORMANCE:时间和性能设置，比如扫描频率、重试次数等等
- FIREWALL/IDS EVASION AND SPOOFING:防火墙绕过和欺骗，比如使用代理，假IP等
- OUTPUT:把扫描接出输出到文件
- MISC: 启用IPv6等等配置

脚本

nmap本身内置了大量的lua脚本，而且还可以自己编写脚本
ls /usr/share/nmap/scripts/ | wc -l
全部清单：https://nmap.org/nsedoc/index.html

例如：
nmap 192.168.142.137 --script http-enum 列举HTTP服务
nmap --script=auth 绕过鉴权
nmap --script=brute 暴力破解
nmap --script=vuln 扫描漏洞

安装metasploitable2 Linux靶机

虚拟机文件在网盘

下载、解压、导入VM

默认用户名密码

msfadmin/msfadmin

修改root密码：

sudo passwd root

使用示例

```
nmap 192.168.142.137 # metasploitable2 Linux
nmap testfire.net    # IBM的一个靶场
```

常用参数

简单扫描
nmap -sP 192.168.142.137

指定端口或范围扫描：
nmap -p0-65535 192.168.142.137

探测操作系统：
nmap -O 192.168.142.137

只进行主机发现，不进行端口扫描
nmap -sn 192.168.40.195/24

IP后面的 /24是什么意思?

掩码的位数。
子网掩码8位，11111111.00000000.00000000.00000000 代表：255.0.0.0（A类IP地址）

子网掩码16位，11111111.11111111.00000000.00000000 代表：255.255.0.0（B类IP地址）

子网掩码24位，11111111.11111111.11111111.00000000 代表：255.255.255.0（C类IP地址）

旁站：和目标网站在同一台服务器但端口不同的其他网站。

C段 ： 和目标服务器IP处在同一个C段的其它服务器。

Zenmap

第一种：Intense scan
第二种：Intense scan plus UDP
第三种：Intense scan,all TCP ports
第四种：Intense scan,no ping
第五种：Ping scan
第六种：Quick scan
第七种：Quick scan plus
第八种：Quick traceroute
第九种：Regular scan
第十种：Slow comprehensive scan

其他扫描工具

在线扫描
http://coolaf.com/tool/port

masscan、nbtscan……

Thank you for watching

无涯老师