CTF_web_study_信息获取

文件读取

端口扫描

一般在知道服务器开放了哪些端口后，就知道服务器开启了哪些服务，然后就可以通过所提供的这些服务的已知漏洞就可进行攻击。

原理：当一个主机向远端一个服务器的某一个端口提出建立一个连接的请求，如果对方有此项服务，就会应答，如果对方未安装此项服务时，即使你向相应的端口发出请求，对方仍无应答，利用这个原理，如果对所有熟知端口或自己选定的某个范围内的熟知端口分别建立连接，并记录下远端服务器所给予的应答，通过查看一记录就可以知道目标服务器上都安装了哪些服务。

常见的端口服务:

端口	协议
21	ftp
22	SSH
23	Telnet
80	web
80-89	web
161	SNMP
389	LDAP
443	SSL心脏滴血以及一些web漏洞测试
445	SMB
512，513，513	Rexec
873	Rsync未授权
1025，111	NFS
1433	MSSQL
1521	Oracle:(iSqlPlus Port:5560,7778)
2082/2083	cpanel主机管理系统登陆 （国外用较多）
2222	DA虚拟主机管理系统登陆 （国外用较多）
2601，2604	zebra路由，默认密码zebra
3128	squid代理默认端口，如果没设置口令很可能就直接漫游内网了
3306	MySQL
3311/3312	kangle主机管理系统登陆
3389	远程桌面
4440	rundeck 参考WooYun: 借用新浪某服务成功漫游新浪内网
5432	PostgreSQL
5900	vnc
5984	CouchDB http://xxx:5984/_utils/
6082	varnish 参考WooYun: Varnish HTTP accelerator CLI 未授权 访问易导致网站被直接篡改或者作为代理进入内网
6379	redis未授权
7001，7002	WebLogic默认弱口令，反序列
7778	Kloxo主机控制面板登录

端口	协议
8000-9090	都是一些常见的web端口，有些运维喜欢把管理后台开在 这些非80的端口上
8080	tomcat/WDCP主机管理系统，默认弱口令
8080，8089，9090	JBOSS
8083	Vestacp主机管理系统 （国外用较多）
8649	ganglia
8888	amh/LuManager 主机管理系统默认端口
9200，9300	elasticsearch 参考WooYun: 多玩某服务器ElasticSearch命令执行漏洞
10000	Virtualmin/Webmin 服务器虚拟主机管理系统
11211	memcache未授权访问
27017，27018	Mongodb未授权访问
28017	mongodb统计页面
50000	SAP命令执行
50070，50030	hadoop默认端口未授权访问

工具

御剑（端口扫描）

nmap

nmap是一款非常强大的主机发现和端口扫描工具，而且nmap运用自带的脚本，还能完成漏洞检测，同时支持多平台。**一般用来攻击靶机**

常用命令：

主机发现	
iR	随机选择目标
-iL	从文件中加载IP地址
-sL	简单的扫描目标
-sn	Ping扫描-禁用端口扫描
-Pn	将所有主机视为在在线，跳过主机发现
-PS[portlist]	（TCP SYN ping） 需要root权限
-PA[portlist]	（TCP ACK ping）
-PU[portlist]	（UDP ping）
-PY [portlist]	（SCTP ping）
-PE/PP/PM	ICMP回显，时间戳和网络掩码请求探测
-PO[协议列表]	IP协议Ping
-n/-R	从不执行DNS解析/始终解析[默认：有时]
--dns-servers	指定自定义DNS服务器
--system-dns	使用OS的dns服务器
--traceroute	跟踪到每个主机的跃点路径
扫描技术	
-sS	使用TCP的SYN进行扫描
-sT	使用TCP进行扫描
-sA	使用TCP的ACK进行扫描
-sU	UDP扫描
-sI	Idle扫描
-sF	FIN扫描
-b<FTP中继主机>	FTP反弹扫描
端口规格和扫描顺序	
-p	扫描指定端口
--exclude-ports	从扫描中排除指定端口
-f	快速模式-扫描比默认扫描更少的端口
-r	连续扫描端口-不随机化
--top-ports	扫描最常用的端口
服务/版本探测	

主机发现	
-sV	探测服务/版本信息
--version-intensity	设置版本扫描强度（0-9）
--version-all	尝试每个强度探测
--version-trace	显示详细的版本扫描活动（用于调试）
操作系统扫描	
-o	启用os检测
输出	
-oN	标准输出
-v	信息详细级别
-oA	同时输出三种主要格式
杂项	
-6	启动Ipv6扫描
-A	启动Os检测，版本检测，脚本扫描和traceroute
-V	显示版本号
-h	帮助信息