Web 系统测试

4.3 Web安全测试—信息收集

河北师范大学软件学院
Software College of Hebei Normal University

目 录

- 域名信息
- 敏感目录
- 端口扫描
- 旁站C段
- 整站分析

收集域名信息

- 收集对应IP地址
- 收集子域名信息
- 注册人信息反查

域名信息

➢收集IP信息

●为什么收集IP信息

- 一个域名对应多个IP，打算做哪台系统的渗透测试，需要先知道其IP地址

●怎样收集IP信息

- ping
- nslookup（域名解析）
- 一些工具网站：site.ip138.com

搜集子域名

- 什么是子域名
  - 子域名，是顶级域名（一级域名或父域名）的下一级
- 为什么搜集子域名
  - 子域名探测可以帮我们发现渗透测试中更多的服务，这将增加发现漏洞的可能性
  - 查找一些用户上较少，被人遗忘的子域名，其上运行的应用程序可能会使我们发现关键漏洞
  - 通常，同一组织的不同域名/应用程序中存在相同的漏洞

搜集子域名

➢怎样收集子域名

- ●在搜索栏输入 site:baidu.com
- ●相关工具
  - layer
  - subDomainsBrute

whois注册人信息查询

- 为什么要查询注册人信息
  - 查看其注册网站的相关信息
- 怎样查询注册人信息
  - 根据已知域名反查，分析出此域名的注册人、邮箱和电话等
  - 使用工具：爱站网、站长工具

搜集Web信息

关键字	说明
site	把搜索范围规定在特定的站点中
intext	正文中存在关键字的网页
intitle	标题中存在关键字的网页
inurl	URL存在关键字的网页
filetype	搜索指定文件类型

搜集Web信息

➢例如：搜索存在敏感信息的网站

- intext:系统登录
- intitle： 系统登录
- inurl:eweb.editor
- intitle:管理登录 filetype:php
  - 查询网页标题中含有“管理登录”，并且为php类型的网站
- intext:Powered by Discuz
  - 正文中存在Discuz关键字

目 录

敏感目录

- 什么是敏感目录
  - 可以被黑客利用的目录，如：后台目录，上传目录等等
- 收集哪些敏感目录
  - robots.txt
  - 后台目录
  - 安装包
  - 上传目录
  - mysql管理接口

敏感目录

➢举例

qufutuan.com/robots.txt

```
User-agent: *
Disallow: /static/
Disallow: /order/
Disallow: /leader/
Disallow: /manage/
Disallow: /forum/
```

敏感目录

- 扫描敏感目录可以使用工具
  - 御剑
  - 爬行菜刀等

目 录

- 域名信息
- 敏感目录
- 端口扫描
- 旁站C段
- 整站分析

常用端口

- FTP ——21
- SSH ——22
- Telnet ——23
- POP3 ——110
- SqlServer ——1433
- Mysql ——3306
- Mstsc ——3389
- Tomcat ——8080
- WebSphere ——9090

端口扫描

- 为什么扫描端口
  - 逐个对一段端口或指定的端口进行扫描。通过扫描结果可以知道一台计算机上都提供了哪些服务，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
- 怎样扫描端口
  - 使用工具：Nmap，portscan，ntscan，telnet

端口扫描—Namp

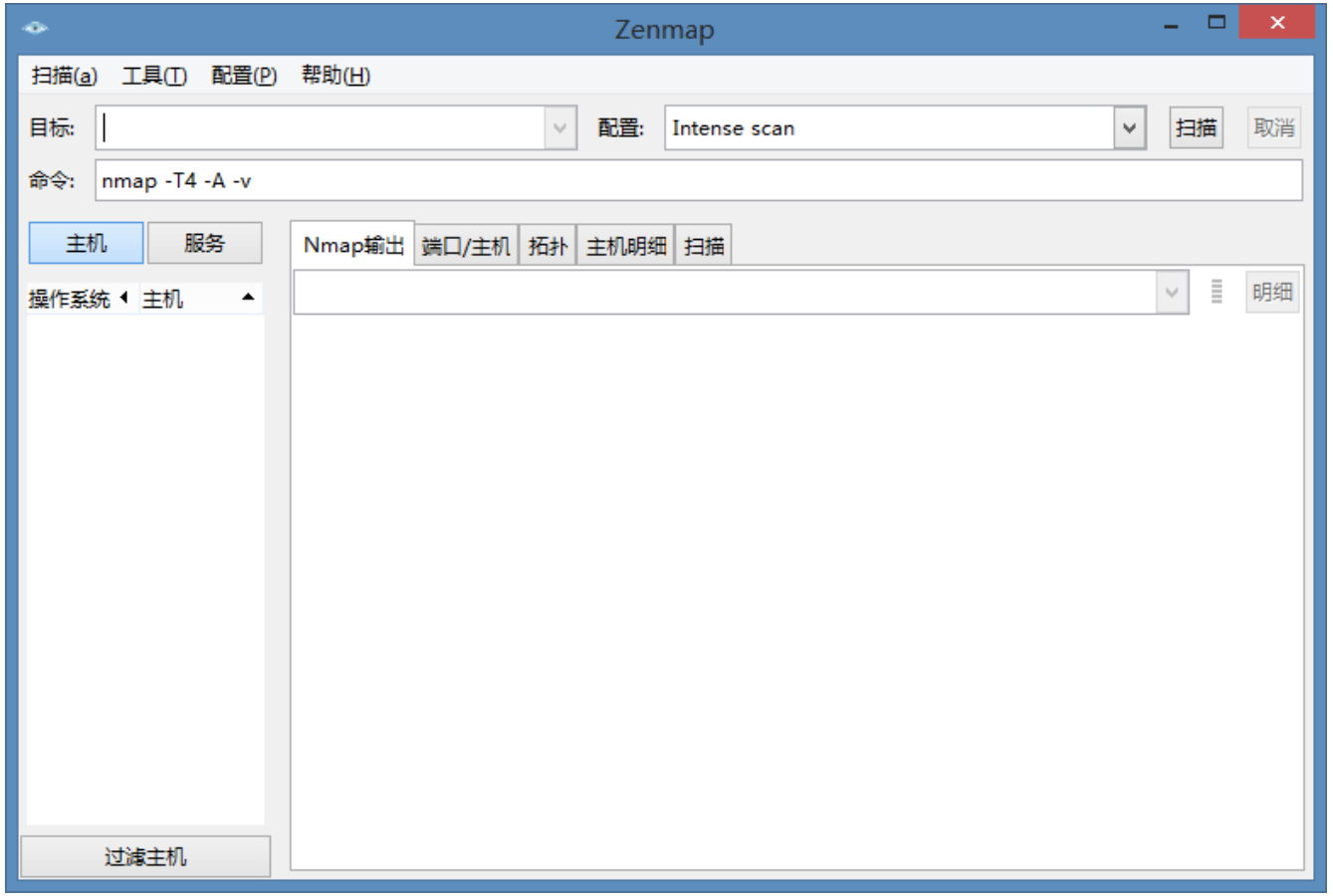
- Nmap，也就是Network Mapper，最早是Linux下的网络扫描和嗅探工具包。nmap是一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端。确定哪些服务运行在哪些连接端

Nmap 初体验

- 安装
- 配置
  - 在环境变量中对系统变量—Path进行编辑，如安装目录为D://Programgram Files\Namp，在Path进行编辑

Nmap启动

- 命令方式
  - cmd---Zenmap
- 图形方式启动
  - 安装目录下，双击zenmap.exe



Nmap扫描方式

(1)TCP connect()端口扫描（-sT参数）

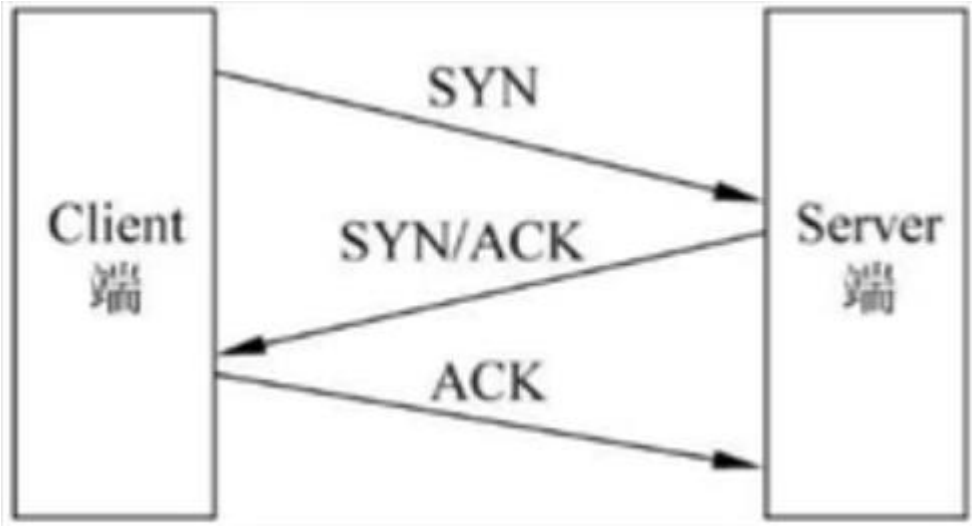
(2) TCP同步（SYN）端口扫描（-sS参数）

(3) UDP端口扫描（-sU参数）

(4) Ping扫描（-sP参数）

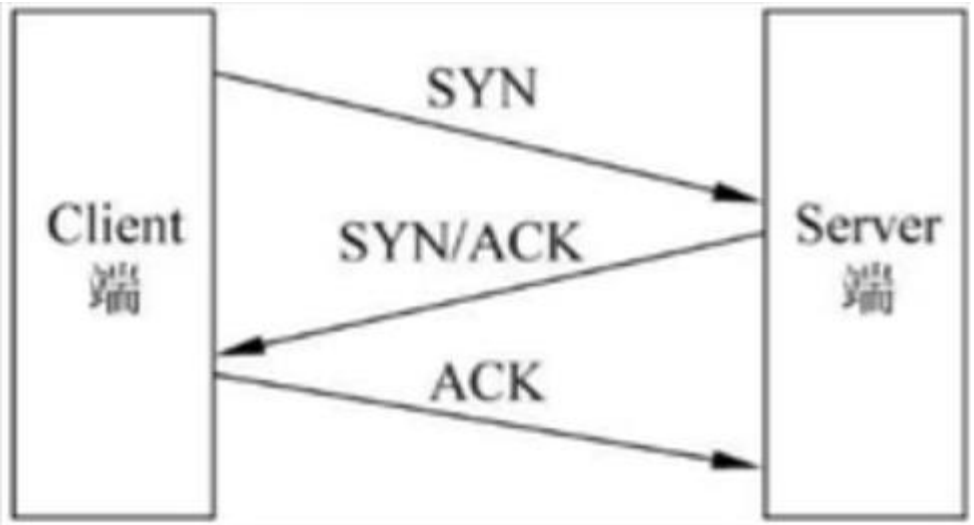
Nmap扫描——TCP Connect扫描

- 普通扫描方法，这种扫描方法的特点
  - 扫描速度快，准确性高，对操作者没有权限上的要求
  - 容易被防火墙和防入侵系统发现
- 运行原理
  - 通过建立TCP的三次握手连接进行信息的传递
  - Client端发送SYN(synchronous建立联机)；
  - Server端返回SYN/ACK，表明端口开放
  - Client端返回ACK (acknowledgement 确认)，表明连接已建立
  - Client端主动断开连接



SYN扫描（TCP同步扫描-sS）

- 这是秘密的扫描方式之一，在Client和Server端，没有形成3次握手，所以没有建立一个正常的TCP连接，因此不被防火墙和日志所记录，一般不会在目标主机上留下任何痕迹，但是这种扫描需要管理员权限



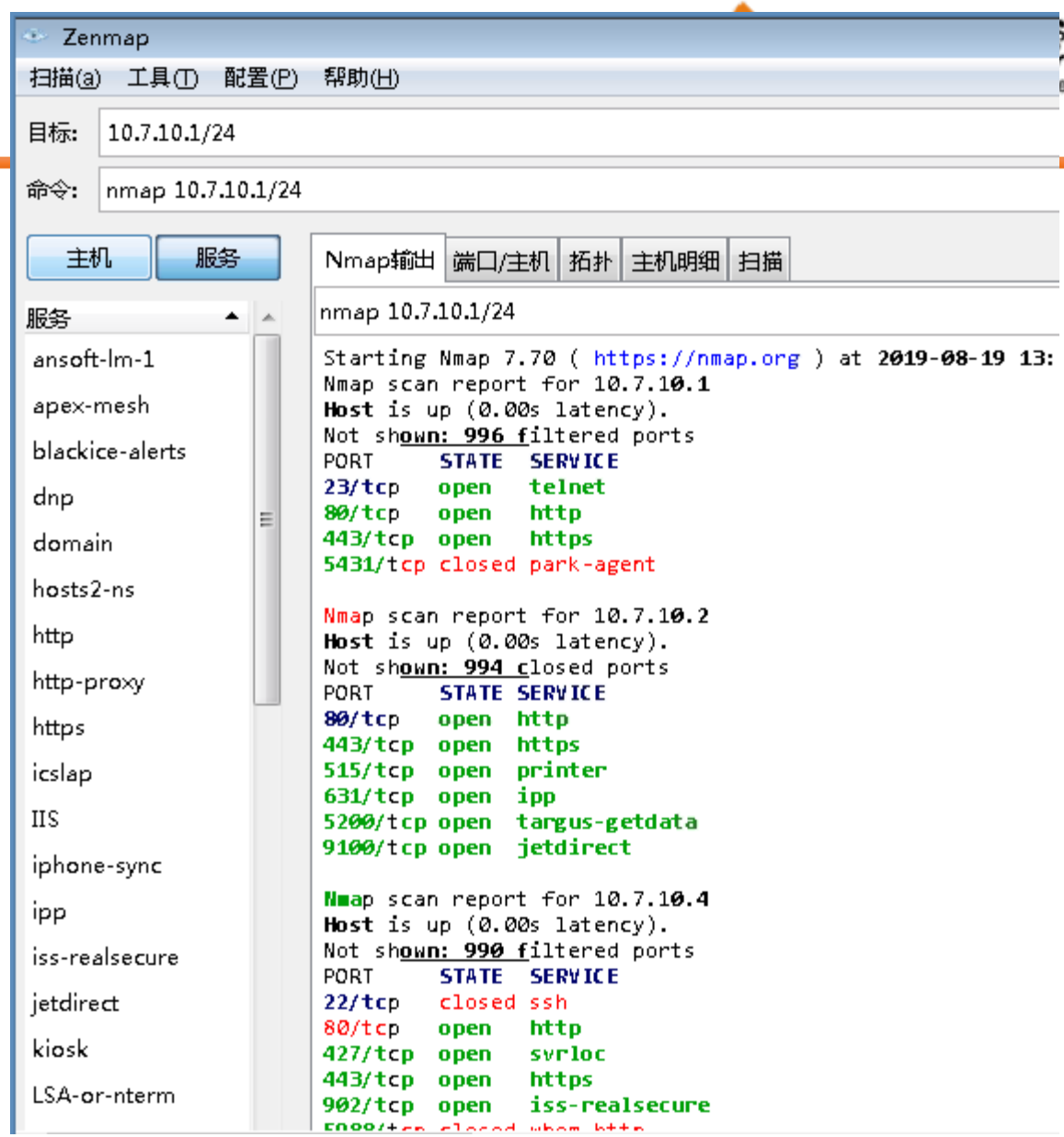
UDP端口扫描（-sU参数）

➢UDP端口扫描

- ●通过普通数据包进行，也是用于扫描对方端口上是否有程序在运行，如果普通个人机器上存在这样的端口，那一般也是系统漏洞
- ●对于UDP来说，不存在监听这个概念，因为它是无连接不可靠的协议，发送数据包过去以后，通常也不会有任何的对等回应
- ●UDP端口扫描主要是检测是否存在ICMP端口不可达数据包。若该数据包出现，则说明对方这一端口上没有程序在监听，或者说该端口不存在漏洞，否则就说明该端口上有程序在监听，或者说存在漏洞

探测主机信息

- 扫描指定IP所开放的端口
  - nmap –sS –p 1-65535 –v 192.168.1.106
- 扫描www.baidu.com C段存活主机
  - nmap –sP www.baidu.com/24
- 指定端口扫描
  - nmap –p 80,1433,22,1521 www.baidu.com


Zenmap
扫描(a) 工具(T) 配置(P) 帮助(H)
目标: 10.7.10.1/24
命令: nmap 10.7.10.1/24
主机 服务
Nmap输出 端口/主机 拓扑 主机明细 扫描
nmap 10.7.10.1/24
服务
ansoft-lm-1
apex-mesh
blackice-alerts
dnp
domain
hosts2-ns
http
http-proxy
https
icslap
IIS
iphone-sync
ipp
iss-realsecure
jetdirect
kiosk
LSA-or-nterm
Starting Nmap 7.70 (https://nmap.org) at 2019-08-19 13:
Nmap scan report for 10.7.10.1
Host is up (0.00s latency).
Not shown: 996 filtered ports
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https
5431/tcp closed park-agent
Nmap scan report for 10.7.10.2
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
515/tcp open printer
631/tcp open ipp
5200/tcp open targus-getdata
9100/tcp open jetdirect
Nmap scan report for 10.7.10.4
Host is up (0.00s latency).
Not shown: 990 filtered ports
PORT STATE SERVICE
22/tcp closed ssh
80/tcp open http
427/tcp open svrloc
443/tcp open https
902/tcp open iss-realsecure

探测主机信息

- 探测主机操作系统
  - nmap –o www.baidu.com
- 全面系统探测
  - nmap –v –A www.baidu.com
- 穿透防火墙进行扫描
  - nmap –Pn –A www.baidu.com

Nmap常用扫描参数及说明

参数	说明
-sT	TCP Connect()扫描，这种方式会在目标主机的日志中记录大批连接请求和错误信息
-sS	半开扫描（目标主机不记录扫描信息）
-sF -sN	秘密FIN数据包扫描，Xmas Tree 、Null扫描模式
-sP	Ping扫描，Nmap在扫描端口时，默认都会使用ping扫描，只有主机存活，Nmap才会继续扫描
-sU	UDP扫描，但UDP扫描是不可靠的
-sA	这项高级的扫描方法通常用来穿过防火墙的规则集
-sV	扫描端口服务版本
-O	启用远程操作系统检测，存在误报

Nmap脚本引擎

➢安装目录下存在Script文件夹，在Script文件夹中存在许多以.nse后缀结尾的文本文件，即Nmap自带的脚本引擎

●扫描Web敏感目录

- nmap –p 80 --script = http-enum.nse www.baidu.com

目 录

旁站C段

- 旁站：同服务器其他站点
- C段：同一网段其他服务器
- 可借助的工具
  - www.webscan.cc

目 录

整站分析

- 脚本格式
- 数据库类型
- 防护情况
- cms类型
- 操作系统

整站分析

- 分析脚本格式
  - url后加 /index.php 或index.asp 或index.jsp
- 查看操作系统类型
  - url中某些字母改为大写，仍然能访问，则判断其是Windows系统，如果不能，则是Linux系统

整站分析

- 查看防护情况：看看有没有软、硬件WAF(Web Application Firewall)
  - URL中输入：http://qufutuan.com/team.php?id=5175 and1=1，查看其是否有拦截，如果有，则说明有防火墙，如果没有拦截则说明没有防火墙
- 查看网站cms
  - www.yunsee.cn

整站分析

➢看容器

- ●抓包，看响应包中 server信息
- ●输入错误url让其报错，查看是哪种Server信息

情报搜集

- www.yunsee.cn

总结

- 域名信息
  - 收集对应IP地址、子域名信息、注册人信息反查
- 敏感目录
  - 哪些是敏感目录，可以借助什么工具扫描
- 端口扫描
  - 常用端口和常用端口扫描工具
- 旁站C段
  - 什么是旁站？什么是C段？
- 整站分析
  - 操作系统、脚本类型、数据库类型、有没有WAF、CMS类型、容器类型等

Question