Web 系统测试

3.3 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

- 搜集子域名
- 搜集Web信息
- 搜集端口、操作系统信息

搜集子域名

- 在搜索栏输入 site:baidu.com

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	一些基本信息
Filetype	URL存在关键字的网页
	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

- 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

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

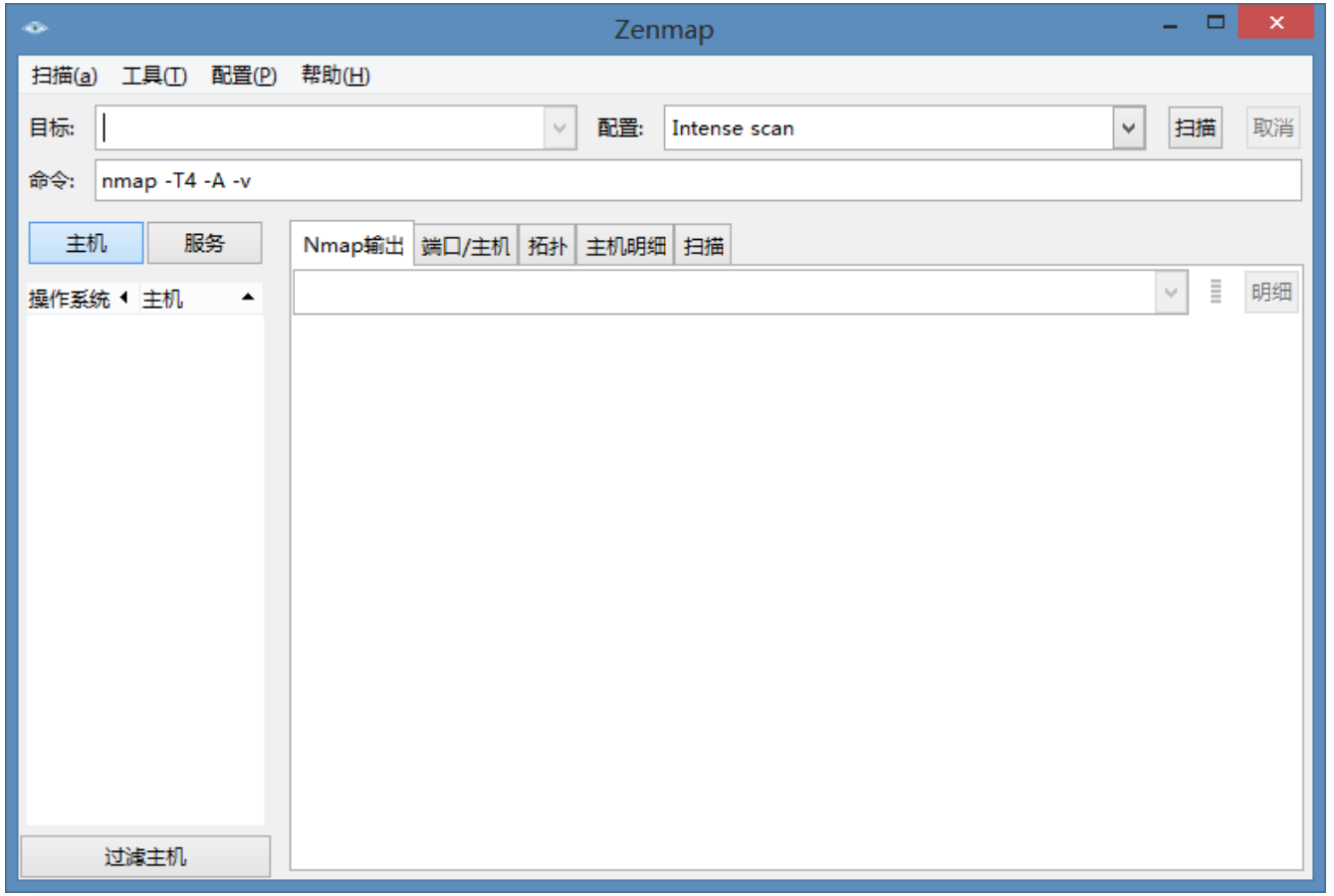
➢命令方式

●CMD---Zenmap

➢图形方式启动

●安装目录下，

双击zenmap.exe



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

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

其他扫描工具

- DrBuster
- Burp Suite

总结

- 信息收集
- 信息收集的工具
  - Nmap
  - Nmap 语法及实例

Question