|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名： | | 学号： | 专业年级： | 班级： |
| 分组： | | 实验室： | 指导教师：郭念 | 实验日期： |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **网络协议分析与攻防技术** | | |
| **实验名称** | 实验五 网络侦察技术 | | |
| **实验目的** | 1. 掌握搜索引擎、Whois数据库、DNS、社会工程学等侦察手段； 2. 了解站点信息查询常用的信息源及搜索工具； 3. 熟悉掌握常见搜索工具的功能及使用技巧； 4. 熟悉联网设备搜索引擎的功能，熟练掌握设备搜索引擎的使用方法。 | | |
| **实验内容** | 1. 站点信息查询   (1) 获得目标站点的相关信息（尽可能包含所有项）：域名服务注册信息，包括：注册商名称及IP地址、注册时间、域名分配的IP地址（段）、注册人联系信息（姓名、邮箱、电话、办公地址）；相关IP地址信息，如DNS、邮件服务器、网关的IP地址。  (2) 站点所属机构的相关信息（尽可能包含所有项）：业务信息、主要负责人信息（姓名、邮箱、电话、办公地址、简历等）、有合作关系的单位名称及网址。   1. 联网设备查询   (1) 查找指定地域内有弱口令、可匿名登录的网络设备（路由器、网关、Server等），并返回其IP地址。  (2) 查找指定地域内网络摄像头，并返回其IP地址。  (3) 实验过程中只允许浏览搜索结果。对搜索到的可远程控制的设备，应禁止学生对这些设备进行远程控制。   1. Sam Spade工具使用 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | Nmap的命令行操作  X-Scan工具的使用 | | |
| **实验环境** | (1) 互联网环境。  (2) 目标域名由教师指定，建议选择有一定影响力的商业公司门户网站的域名或使用本单位门户网站域名。  (3) 搜索引擎Shodan或ZoomEye。  (4) 搜索地域（国家、城市、区、街道、经纬度等）由教师指定或学生自主确定。 | | |
| **实验的实施阶段** | **实验步骤及实验结果** | 1. 百度高级搜索    1. 在百度搜索标题中含有“网络侦察”的Word文档，实验过程截图如下：      * 1. 在河南大学官网：[www.henu.edu.cn](http://www.henu.edu.cn)范围内搜索包含软件学院的信息，实验过程截图如下：      * 1. 在百度搜索河南大学结果中过滤掉“软件学院”的信息，实验过程截图如下：      1. 站点信息查询（自主指定）   2.1 在互联网数字分配机构的Whois数据库（https://www.iana.org/whois）查询新浪网www.sina.com.cn的域名注册机构，获得域名服务注册信息包括：注册商名称及IP地址、注册时间、域名分配的IP地址（段）、注册人联系信息（姓名、邮箱、电话、办公地址），实验过程截图如下：    2.2 在查询结果中找到注册机构域名，继续查询新浪网的域名，查询获得目标站点的相关信息（尽可能包含所有项）：相关IP地址信息，如DNS、邮件服务器、网关的IP地址。实验过程截图如下：    2.3 打开新浪网，收集该站点所属机构的相关信息（尽可能包含所有项）：业务信息、主要负责人信息（姓名、邮箱、电话、办公地址、简历等）、有合作关系的单位名称及网址。实验过程截图如下：     1. 联网设备查询   **注意：实验过程中只允许浏览搜索结果。对搜索到的可远程控制的设备，应禁止学生对这些设备进行远程控制。**  搜索语法   * **hostname**：搜索指定的主机或域名，例如 **hostname:"google"** * **port**：搜索指定的端口或服务，例如 **port:"21"** * **country**：搜索指定的国家，例如 **country:"CN"** * **city**：搜索指定的城市，例如 **city:"Hefei"** * **org**：搜索指定的组织或公司，例如 **org:"google"** * **isp**：搜索指定的ISP供应商，例如 **isp:"China Telecom"** * **product**：搜索指定的操作系统/软件/平台，例如 **product:"Apache httpd"** * **version**：搜索指定的软件版本，例如 **version:"1.6.2"** * **geo**：搜索指定的地理位置，参数为经纬度，例如 **geo:"31.8639, 117.2808"** * **before/after**：搜索指定收录时间前后的数据，格式为dd-mm-yy，例如 **before:"11-11-15"** * **net**：搜索指定的IP地址或子网，例如 **net:"210.45.240.0/24"**   **Shodan黑客搜索引擎（入门教程）：https://zhuanlan.zhihu.com/p/267202589**   * 1. 打开Shodan（www.shodan.io），注册一个新用户，查找指定地域内有弱口令、可匿名登录的网络设备（路由器、网关、Server等），并返回其IP地址。实验过程截图如下：      * 1. 继续查找指定地域内网络摄像头，并返回其IP地址。实验截图如下：      * 1. 继续查找某地范围内的交通信号，实验截图如下：     3.4 搜索思科公司在全世界的路由器设备，实验过程截图如下：(3)     1. Sam spade的使用   4.1 下载并安装Sam Spade，安装完毕后打开该软件，实验过程截图如下：    4.2 在搜索框 输入：baidu.com，按右侧的“Go”按钮。实验过程截图如下：    4.3 点击左侧工具栏的ping按钮，实验过程截图如下：    4.4 点击左侧工具栏的Whois按钮，实验过程截图如下：    4.5 点击左侧工具栏的IPBlocks按钮，实验过程截图如下：    4.6 点击左侧工具栏的Trace按钮，实验过程截图如下： | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | **【实验思考】**   * + - 1. 网络侦察的防御方法有哪些？   加强培训、实施主动防护、尝试网络欺骗防御工具、开发从设计开始的反侦察服务，以及重新考虑隐私概念。配置防火墙，阻断ICMP以及任何未知协议数据包，过滤异常的数据包和请求。检测识别网络侦察流量，然后有针对性地对流量进行处理，处理方法包括阻断、限流、使用虚假响应。 | | |