渗透测试工程师技术实战课

渗透工具篇渗透工具篇1 第1-2课

教学目标

★ 能够掌握侦查相关的Google hack、nmap、DirBuster等工具

★ 理解侦查的重要性

●Google hacking

★ 条件：科学上网　ss/ssr/v2ray+节点

★ 使用Google搜索引擎通过特定语法或自定义语法来查找网站配置中的安全漏洞

★ https://www.google.com 可实现站内搜索

●Google hacking

★ 基本逻辑以及操作符

- 查询是不区分大小写（模糊查询）
- 精准搜索要带上半角引号
- 通配符 “*”
- 布尔查询
- ...

●Google hacking

标题/正文中搜索

- intitle或allintitle
- intext或alltext

Index of /admin

Name	Last modified	Size	Description
Parent Directory		-	
admin.php	2017-08-02 10:17	39K	
files/	2018-06-05 17:43	-	

●Google hacking

★ 常见运算符解释

- site 把搜索精确到特定的网站
- filetype 搜索特定后缀的文件
- inurl: 用于搜索网页上包含的URL

Password Reset - Pocketmags.com

翻译此页

Pocketmags.com password reminder, delivering magazines and newspapers to PC, Mac, iPhone, iPad and Android.

gmail_videoCall_VideoNotWorking.log - FreeSWITCH

_videoC... ▾ 翻译此页

D83752F5" xmlns:ses="http://www.google.com/session"> <ses:candidate address=' port="62964" name="rtp" username="dANP3HWyv " ...

</p:transport></jin:content></jin:jingle>
<ses:session type="candidates" id="c1380521088" initiator="sanjay.sanjaysoni@gmail.com/gmail.D83752F5" xmlns:ses="http://www.goog
<ses:candidate address= port="62964" name="rtp" username="dANP3HWyv password="
</ses:session></iq>

●Google hacking

攻击：

- 查找目录列表
- 目录遍历技术
- 配置文件
- 查找文件
- office文档
- 数据库挖掘

●Google hacking

查找漏洞寻找目标：

- 查找漏洞代码
- 查找公开漏洞的网站
- 查找易受攻击的目标

●Google hacking

保护自己免受google骇客攻击

- **目录列表和丢失的索引文件**

.htaccess 可以来防止目录的内容未授权的访问，但是不当的配置还会让这个文件可见甚至可读

在 apache 的服务器上可以通过 httpd.conf文件中的单词indexs前加一个连字符或者减号来禁止目录列表

robots.txt

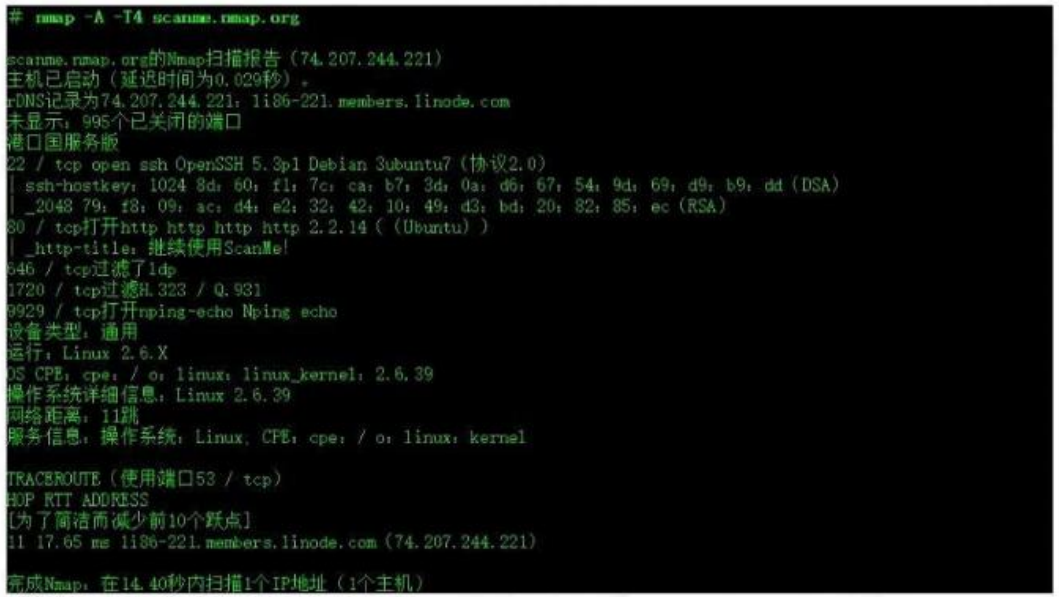
●Google hacking

1.检查所有的文档能否被Google搜索到，避免敏感文件能出现在公众的视野中
2.选择一个强大的自动化工具来扫描你网站上是否有信息的泄露
3.不要使用默认的登录入口，以防止登录入口被hack猜解
4.关闭数据库的远程管理工具
5.删除明显的显示软件版本的信息
6.配置服务器只能下载特定的文件类型（白名单比黑名单要简单有效得多）
7.正确的配置你的服务器，不要抱有侥幸心理，任何的松懈带来的灾难是巨大的
8.不要把源码的备份放在未经授权就能访问的地方，并且及时删除网站上的无用的备份文件
9.不要使用弱密码，防止攻击者轻易攻破后台
10.登录请加上强度相对较高的验证手段，防止攻击者采用爆破的手段
11.关闭服务器不必要的端口
12.请不要使用网站上的任何信息作为密码，否则都属于容易爆破的类型
13.备份的源代码请经过专业的混淆，防止被下载之后轻易读取到内容
14.及时更新服务器的系统，修复潜在的漏洞
15.安装正规的安全防护软件，如"安全狗"

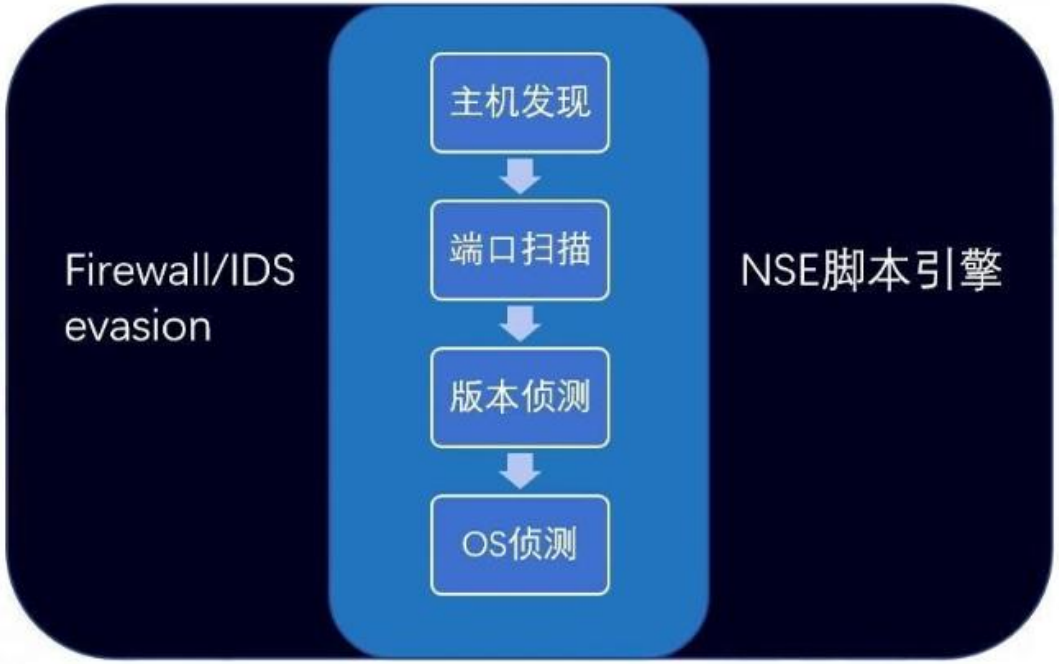
●Nmap

什么是Nmap?

- Nmap是一种用于网络探索和安全审计的开源工具。它旨在快速扫描大型网络，Nmap用于列举网络主机清单、管理服务升级调度、监控主机或服务运行状况。



- 功能?



●Nmap

- zenmap


Zenmap
扫描(a) 工具(T) 配置(P) 帮助(H)
目标:
配置: Intense scan
扫描
取消
命令: nmap -T4 -A -v
主机
服务
Nmap输出 端口/主机 拓扑 主机明细 扫描
操作系统 主机
明细
关于Nmap和Zenmap
Zenmap 7.70
Copyright 2005-2016 Insecure.Com LLC
Nmap
Nmap是一款免费开源的软件，用于网络探测和安全审计。
Zenmap
Zenmap是一款跨平台图形化Nmap前端，也是一款结果浏览器。最初由Umit衍生而来。
Umit
Umit开发团队
Umit是Nmap的图形界面，是Nmap/Google Summer of Code的一个子项目。
对于中文翻译有任何建议或意见，请截图发送至: jerrynwin 0 gmail com, 谢谢!
Close
过滤主机

命令行模式

- nmap targethost 可以确定目标主机在线情况及端口基本状况。
- nmap -T4 -A -v targethost 完整全面的扫描

主机发现的用法

- -sn: Ping Scan 只进行主机发现，不进行端口扫描。
- -Pn: 将所有指定的主机视作开启的，跳过主机发现的过程。
- -PS/PA/PU/PY[portlist]: 使用TCPSYN/ACK或SCTP INIT/ECHO方式进行发现
- -PE/PP/PM: 使用ICMP echo, timestamp, and netmask 请求包发现主机。
- -PO[protocollist]: 使用IP协议包 探测对方主机是否开启

端口扫描原理

- 端口扫描是 Nmap最基本最核心的功能，用于确定目标主机的 TCP/UDP端口的开放情况。默认情况下，Nmap会扫描 1000个最有可能开放的 TCP端口。
  - open：端口是开放的。
  - closed：端口是关闭的。
  - filtered：端口被防火墙 IDS/IPS屏蔽，无法确定其状态。
  - unfiltered：端口没有被屏蔽，但是否开放需要进一步确定。
  - -sS/sT/sA/sW/sM:指定使用 TCP SYN/Connect()/ACK/Window/Maimon scans的方式来对目标主机进行扫描。
  - -p <port ranges>: 扫描指定的端口

版本侦测

用于确定目标主机开放端口上运行的具体的应用程序及版本信息

- -sV: 指定让Nmap进行版本侦测
- --version-intensity <level>: 指定版本侦测强度（0-9），默认为 7。数值越高，探测出的服务越准确，但是运行时间会 比较长。
- --version-light: 指定使用轻量侦测方式 (intensity 2)
- --version-all: 尝试使用所有的 probes进行侦测 (intensity 9)
- --version-trace: 显示出详细的版本侦测过程信息。

OS侦测

操作系统侦测用于检测目标主机运行的操作系统类型及设备类型等信息。 Nmap拥有丰富的系统数据库 nmap-os-db，目前可以识别 2600多种操作系统与设备类型。

- -O: 指定 Nmap进行 OS侦测
- --osscan-limit: 限制Nmap只对确定的主机的进行 OS探测
- --osscan-guess: 大胆猜测对方的主机的系统类型。由此准确性会下降不少，但会尽可能多为用户提供潜在的操作系统。

Nmap高级用法

防火墙/IDS规避

- -f; --mtu <val>: 指定使用分片、指定数据包的MTU.
- -D <decoy1,decoy2[,ME],...>: 用一组IP地址掩盖真实地址，其中ME 填入自己的IP地址。
- -S <IP_Address>: 伪装成其他IP地址
- --ip-options <options>: 使用指定的IP选项来发送数据包。
- --spoof-mac <mac address/prefix/vendor name>: 伪装MAC地址
- --badsum: 使用错误的checksum来发送数据包（正常情况下，该类数据包被抛弃，如果收到回复，说明回复来 自防火墙或IDS/IPS）

NSE脚本引擎

- 网络发现（Network Discovery）
- 更加复杂的版本侦测（例如skype软件）
- 漏洞侦测(Vulnerability Detection)
- 后门侦测(Backdoor Detection)
- 漏洞利用(Vulnerability Exploitation)

NSE脚本引擎

- -sC: 等价于 --script=default，使用默认类别的脚本进行扫描。
- --script=<Lua scripts>: <Lua scripts>使用某个或某类脚本进行扫描，支持通配符描述
- --script-args=<n1=v1,[n2=v2,...]>: 为脚本提供默认参数
- --script-args-file=filename: 使用文件来为脚本提供参数
- --script-trace: 显示脚本执行过程中发送与接收的数据
- --script-updatedb: 更新脚本数据库
- --script-help=<Lua scripts>: 显示脚本的帮助信息，其中<Luascripts>部分可以逗号分隔的文件或脚本类别。

●DirBuster

使用DirBuster寻找敏感文件和目录

- DirBuster 是一款安全工具，通过暴力或者表单进行来发现Web服务器中现有文件和目录。我们将在文中使用它来搜索特定的文件和目录列表。

准备

- 我们要使用一个文本文件，其中包含我们要用DirBuster来查找的文件列表。
- 创建一个包含这些敏感文件和目录内容的文本文件dir_dictionary.txt

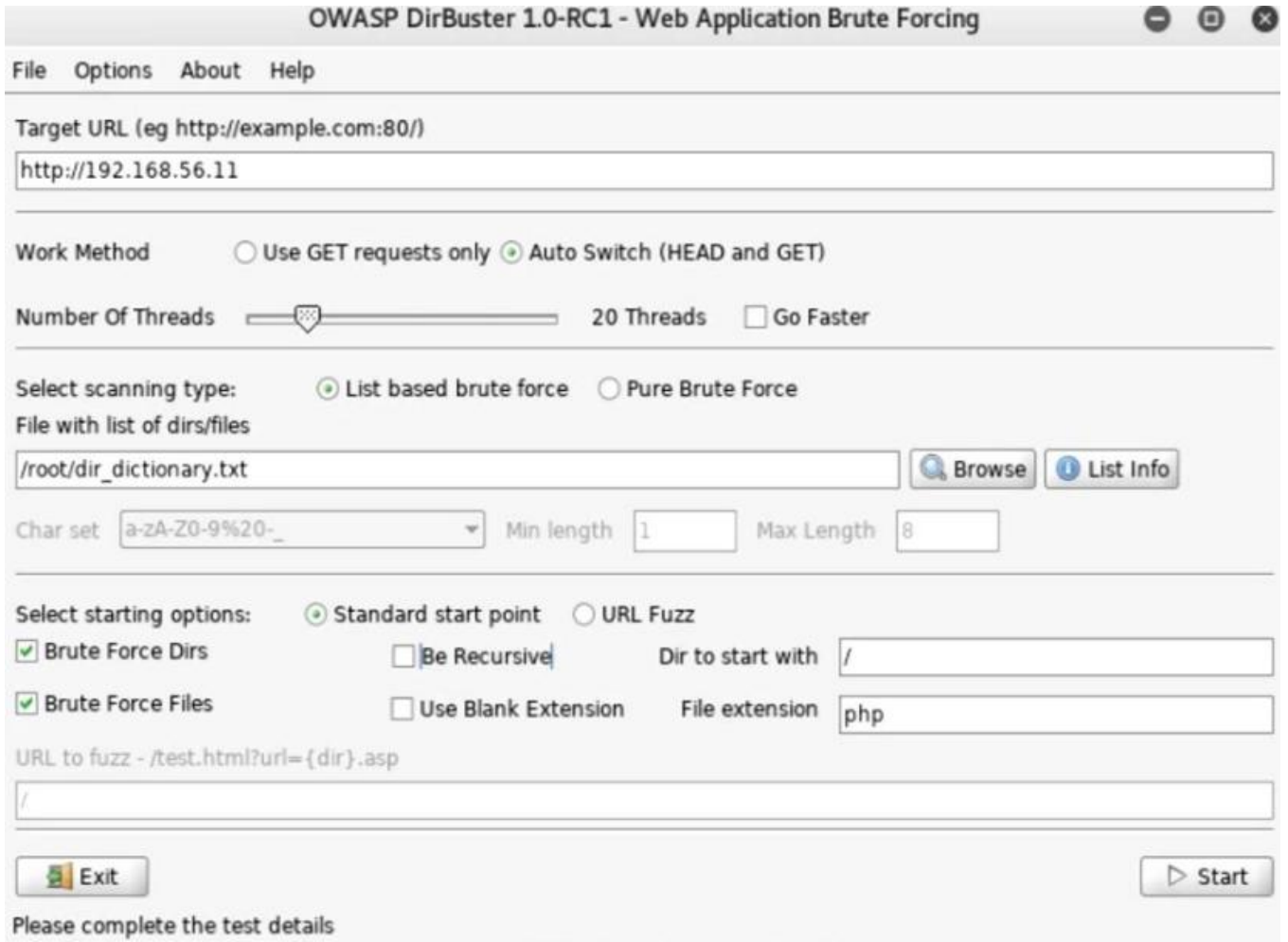
●DirBuster

步骤：

- 在终端下输入 dirbuster 打开这个软件
- 在DirBuster窗口中，将目标URL设置为http://192.168.56.11/.
- 将线程数设置为20，以获得不错的测试速度。
- 选择基于列表的暴力破解，然后单击“浏览”。
- 在浏览窗口中，选择我们刚刚创建的文件（dir_dirtionary.txt）
- 取消选中Be Recursive选项.
- 对于这个配置，我们将其余选项保留为默认值：

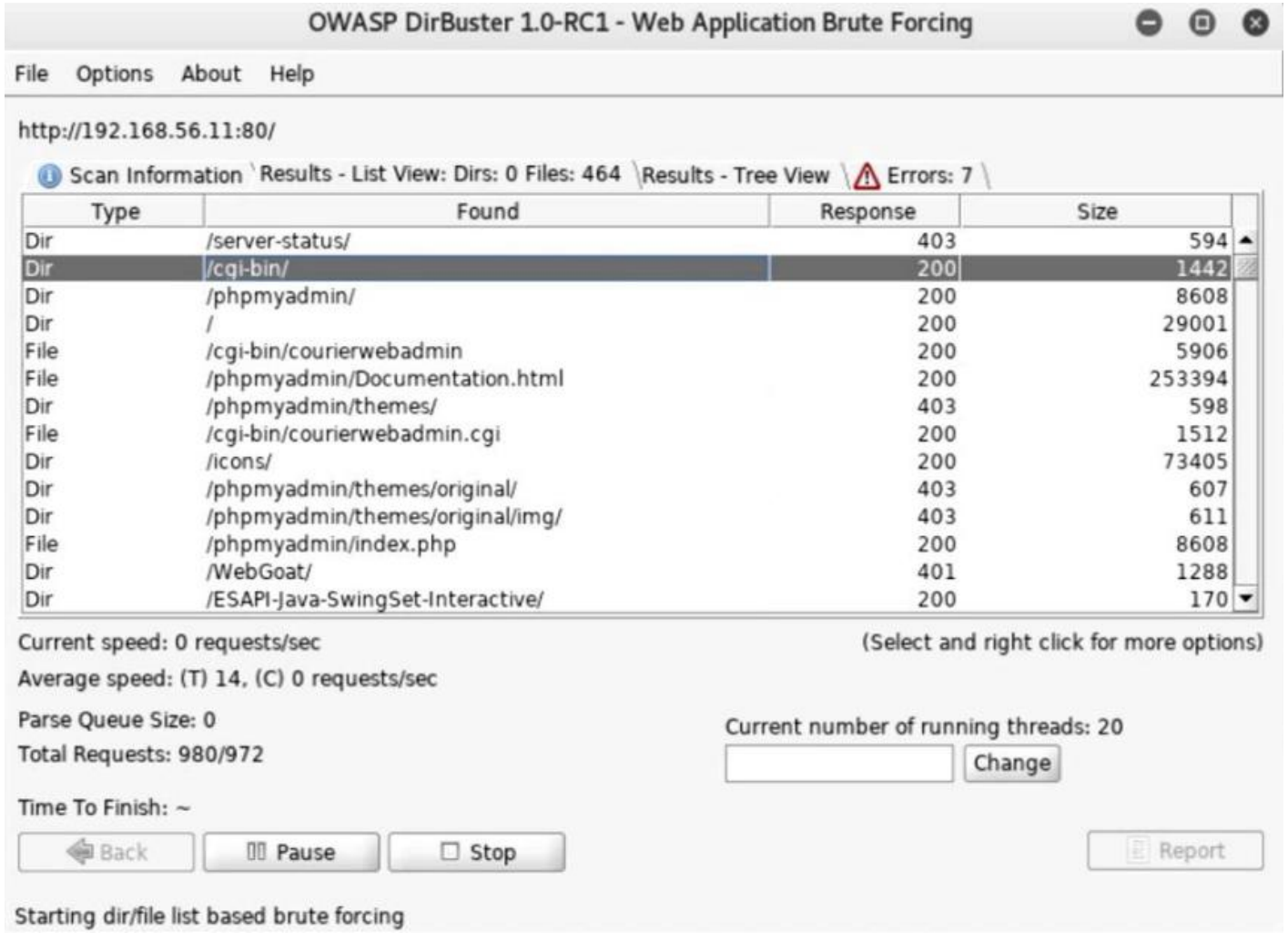
●DirBuster

- 点击：start



●DirBuster

- 结果：



●DirBuster

DirBuster使用服务器的响应代码。最常见的响应如下所示：

- 200 ok：文件存在
- 404 找不到404文件：服务器中不存在该文件
- 301 301永久移动：这是重定向到给定的URL
- 401 Unauthorized:访问此文件需要身份验证
- 403 Forbidden：请求有效但服务器拒绝响应

谢谢观赏