

# Kali linux渗透测试

苑房弘 FANGHONG.YUAN@163.COM

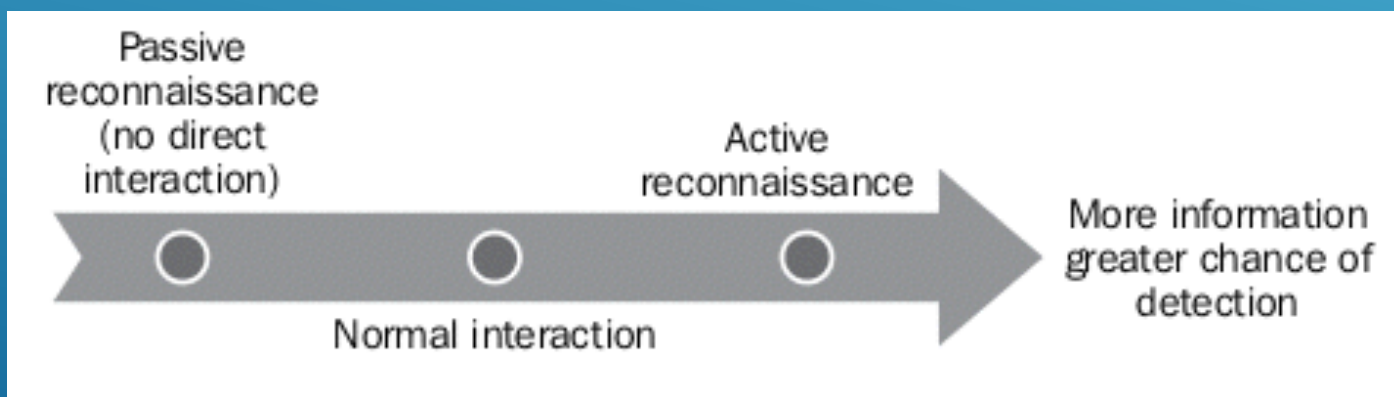


# 第六章 被动信息收集




# 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

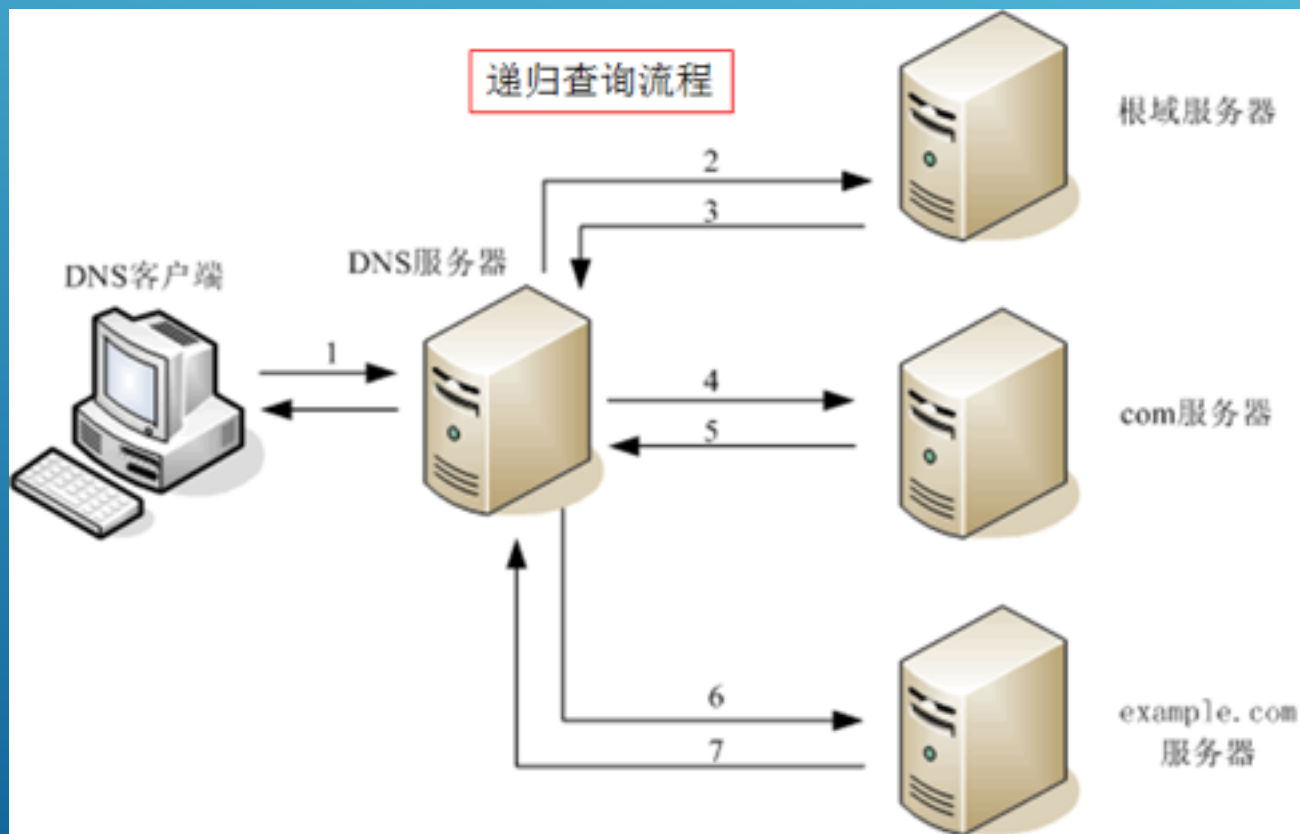
- IP地址段
  - 域名信息
  - 邮件地址
  - 文档图片数据
  - 公司地址
  - 公司组织架构
  - 联系电话 / 传真号码
  - 人员姓名 / 职务
  - 目标系统使用的技术架构
  - 公开的商业信息
- 
- Several white lines of varying lengths and orientations are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

# 信息用途

- 用信息描述目标
  - 发现
  - 社会工程学攻击
  - 物理缺口
- 
- Several white lines of varying lengths and orientations are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

# 信息收集——DNS

- 域名解析成IP地址
  - 域名与FQDN的区别
  - 域名记录：A、CNAME、NS、MX、PTR



# DNS信息收集——NSLOOKUP

- nslookup www.sina.com
- server
- type=a、mx、ns、any
- nslookup -type=ns example.com 156.154.70.22

# DNS信息收集——DIG

- `dig @8.8.8.8 www.sina.com mx`
- `dig www.sina.com 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 @ns3.dnsv4.com`
- 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 @ns1.example.com example.com axfr`
- `host -T -l sina.com 8.8.8.8`

# DNS字典爆破


- `fierce -dnsserver 8.8.8.8 -dns sina.com.cn -wordlist a.txt`
- `dnsdict6 -d4 -t 16 -x sina.com`
- `dnsenum -f dnsbig.txt -dnsserver 8.8.8.8 sina.com -o sina.xml`
- `dnsmap sina.com -w dns.txt`
- `dnsrecon -d sina.com --lifetime 10 -t brt -D dnsbig.txt`
- `dnsrecon -t std -d sina.com`

# DNS注册信息

- Whois
- `whois -h whois.apnic.net 192.0.43.10`

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

# 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
- 
- Several white lines of varying lengths and slopes are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

# SHODAN

- 搜索联网的设备
- Banner: http、ftp、ssh、telnet
- <https://www.shodan.io/>
  - <http://1.179.177.109:81/index.htm>
- 常见filter:
  - net (192.168.20.1)
  - city
  - country (CN、US)
  - port (80、21、22、23)
  - os
  - Hostname (主机或域名)

# 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
- 塞班司法案的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"`
- `inurl:ftp "password" filetype:xls site:baidu.com`
- `Service.pwd`
  
- `http://exploit-db.com/google-dorks`

# YANDEX

- 世界第四大搜索引擎——俄罗斯
- <https://www.yandex.com/>



# RECON-NG

- 全特性的web侦察框架
- 基于Python开发



# 用户信息

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

# MELTAGO

- 申请账号
- 登陆使用

# 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


- Web信息搜索框架
- 命令格式与msf一致
- 基于python开发
- 使用方法：
  - 模块
  - 数据库
  - 报告

# RECON-NG

- 全局选项
  - USER-AGENT
  - Proxy
  - Workspace
  - Snapshot
- Show schema
- Help
- Query 数据库
  - `Select * from hosts where host like '%baidu.com%' order by ip_address`



# RECON-NG

- DNS查询
    - Google
    - Baidu
    - Bing
    - Yahoo
    - Brute force
  - 解析IP地址（查询数据库）
  - 联系人
  - 报告
  - API
- 
- Several white lines of varying lengths and angles are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

# Q & A

