Kali Linux 滲透測試方法

The quieter you become， the more you are able to hear

WHOAMI

- 姓名：苑房弘
- 职务：电商公司 安全部经理
- 经验：10年安全技术从业经验，2 年计算机技术培训师
- 自评：跟随安全行业发展不断学习的一名工程师
- 认证：CISSP、CIW、MCSE、CCNP
- 邮箱：fanghong.yuan@163.com

目录

安全问题的根源

- 从更加宏观的角度来了解安全
  - 概览安全体系的知识结构
  - 明确渗透测试在其中的位置

- 最近一次技术交流引发的思考
- 分层思想的利弊
  - 片面的认识安全
  - 只追求功能实现
  - 人层是问题的根源
  - 静态的分层不能满足需要

软件安全生命周期

需求 → 设计 → 编码 → 测试 → 上线 → 运维

安全需求 → 系统架构 → 编码规范 → 代码审计 → 部署规范 → 环境审计

安全意识教育

渗透测试

渗透测试的意义

- 安全建设
  - 周期长
  - 投入大
  - 效果不易测量
- 渗透测试
  - 从问题出发检查系统安全
  - 用黑客的视角审视系统
  - 在资源有限的情况下效率更高
- 渗透测试的目标是达到安全
  - ≠ 恶意黑客

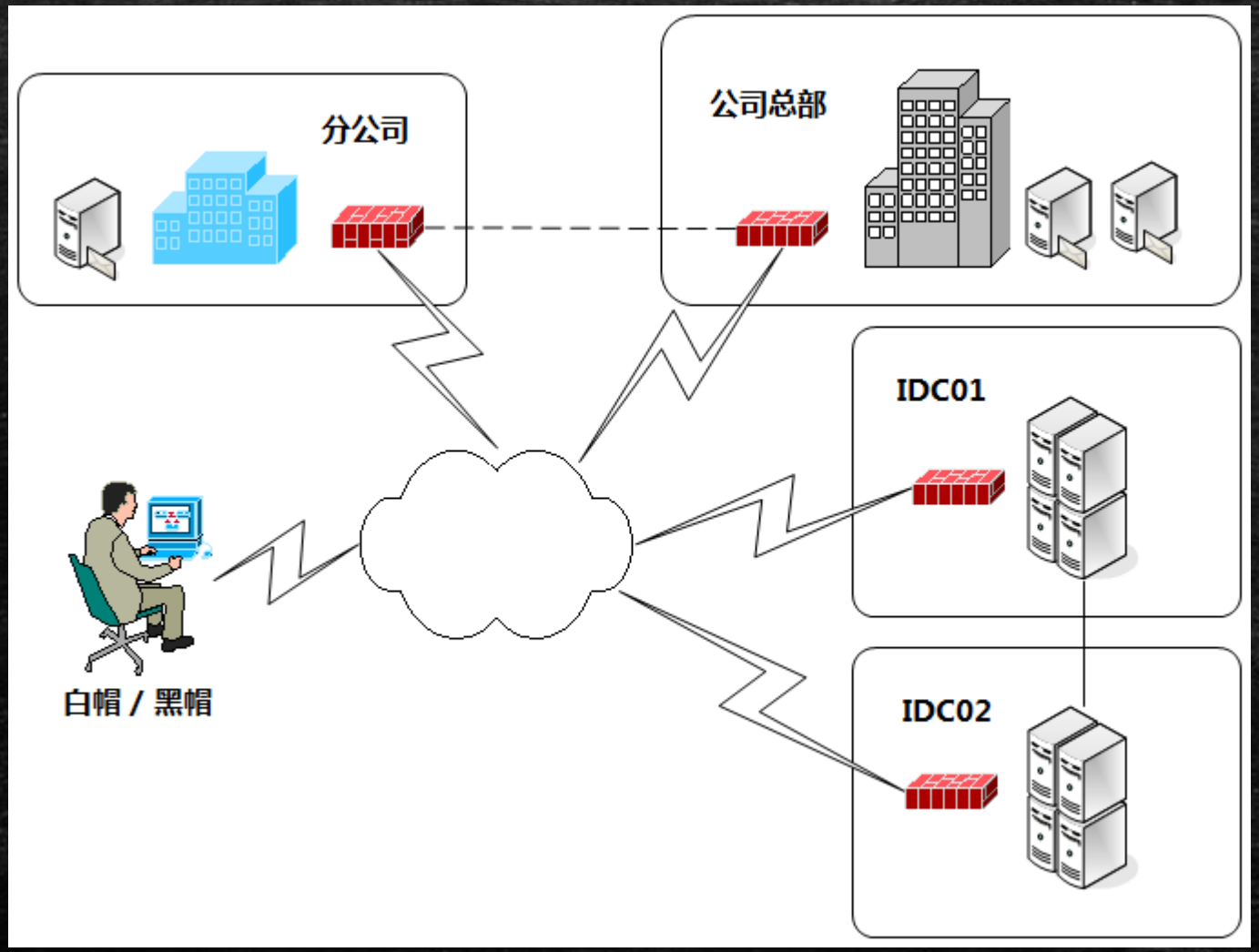
Kali Linux简介

- 前身是BackTrack（BT5r3）
- 黑帽 / 白帽 专用的操作系统
- 渗透测试和安全审计平台
- 安全工具的军火库
- 目前包含工具600+
- 支持包括ARM的多平台
- 工具党

渗透测试标准 PETS

1. 前期沟通
2. 信息收集
3. 威胁建模
4. 漏洞分析
5. 渗透攻击
6. 后渗透测试
7. 测试报告

渗透测试场景



渗透测试标准 PETS

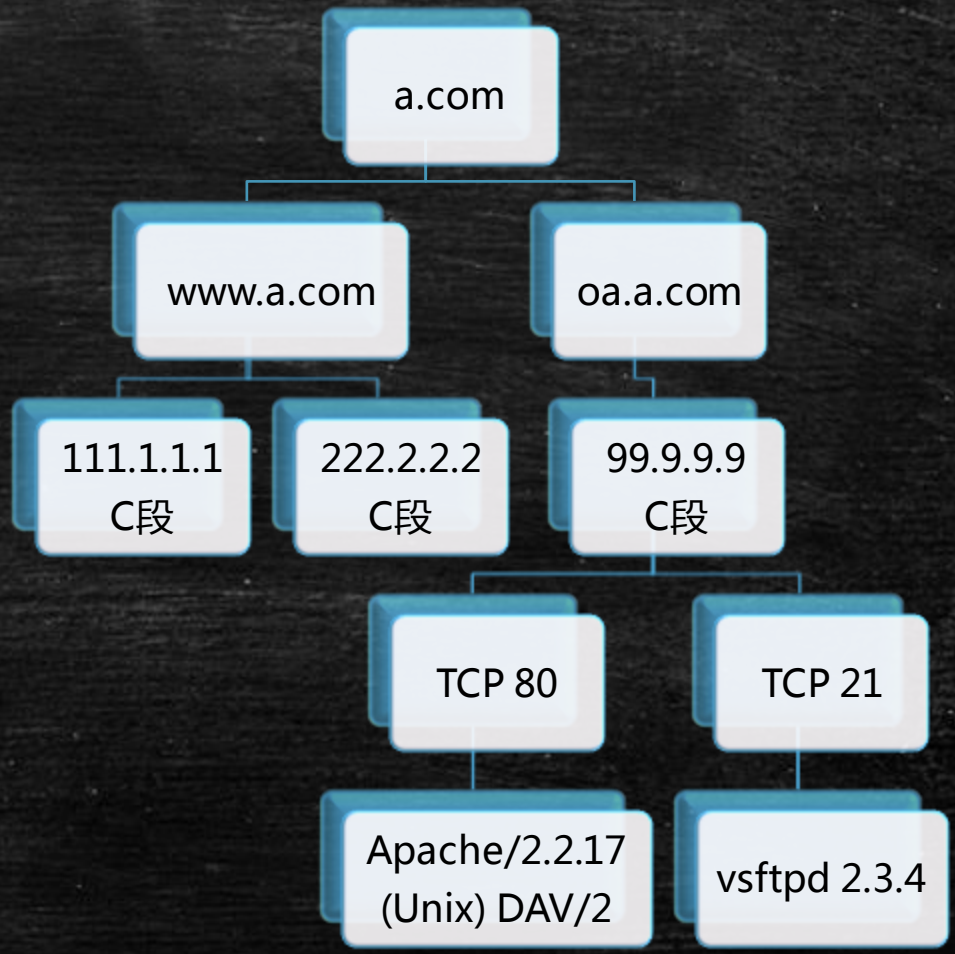
1. 前期沟通
2. 信息收集
3. 威胁建模
4. 漏洞分析
5. 渗透攻击
6. 后渗透测试
7. 测试报告

被动信息收集 OSINT

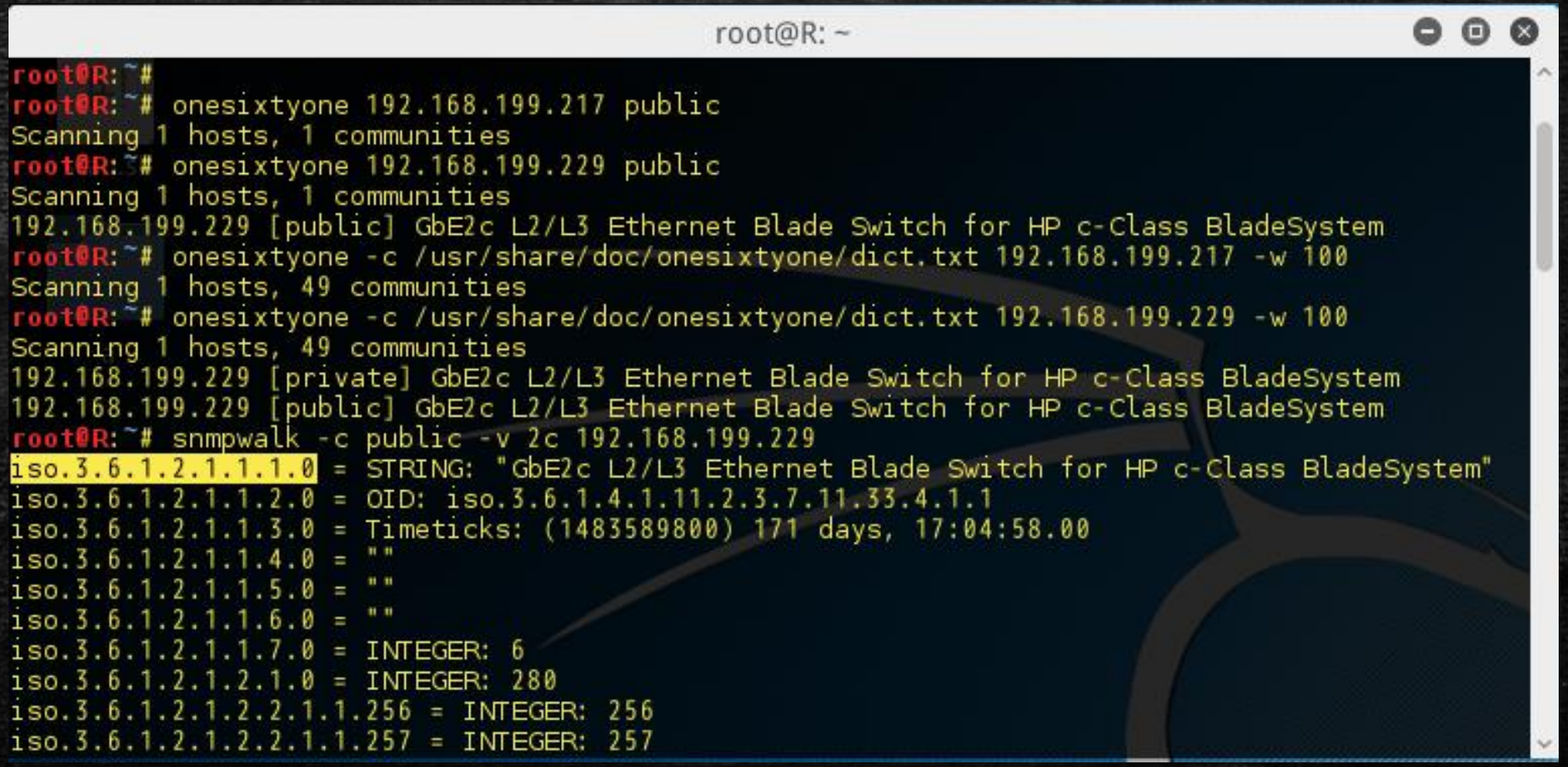
- 域名、邮箱、人员、地址
  - Nslookup、dig、Whois
  - Fierce
  - Dnsrecon
- 搜索引擎
  - Shodan
  - Google
- Metadata
- 专属密码字典
  - Cupp

主动信息收集

- 扫描IP地址段
  - NMAP
- 其他服务扫描
  - SNMP、SMB、SMTP、WEB
- 识别防护机制
  - LBD
  - Wafwoof
  - Fragroute
  - Nmap



主动信息收集


root@R: ~
root@R:~#
root@R:~# onesixtyone 192.168.199.217 public
Scanning 1 hosts, 1 communities
root@R:~# onesixtyone 192.168.199.229 public
Scanning 1 hosts, 1 communities
192.168.199.229 [public] GbE2c L2/L3 Ethernet Blade Switch for HP c-Class BladeSystem
root@R:~# onesixtyone -c /usr/share/doc/onesixtyone/dict.txt 192.168.199.217 -w 100
Scanning 1 hosts, 49 communities
root@R:~# onesixtyone -c /usr/share/doc/onesixtyone/dict.txt 192.168.199.229 -w 100
Scanning 1 hosts, 49 communities
192.168.199.229 [private] GbE2c L2/L3 Ethernet Blade Switch for HP c-Class BladeSystem
192.168.199.229 [public] GbE2c L2/L3 Ethernet Blade Switch for HP c-Class BladeSystem
root@R:~# snmpwalk -c public -v 2c 192.168.199.229
iso.3.6.1.2.1.1.1.0 = STRING: "GbE2c L2/L3 Ethernet Blade Switch for HP c-Class BladeSystem"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.11.2.3.7.11.33.4.1.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (1483589800) 171 days, 17:04:58.00
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = ""
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 6
iso.3.6.1.2.1.2.1.0 = INTEGER: 280
iso.3.6.1.2.1.2.2.1.1.256 = INTEGER: 256
iso.3.6.1.2.1.2.2.1.1.257 = INTEGER: 257

渗透测试标准 PETS

1. 前期沟通
2. 信息收集
3. 威胁建模
4. 漏洞分析
5. 渗透攻击
6. 后渗透测试
7. 测试报告

威胁建模

- 传统威胁建模方法
  - 资产 / 攻击者（ Agents/Community ）
- PETS标准威胁建模方法
  - 商业资产：主要资产、次要资产
  - 商业流程：技术支持、资产管理、人力资源、第三方
  - 威胁主体：内部、外部
  - 威胁能力：威胁主体的能力，威胁的可能性
  - 企业专有的威胁模型，而非通常的技术建模
- 动机建模
- 影响建模

内部	外部
员工	商业合作伙伴
经理	行业竞争者
管理员	有组织犯罪
研发	脚本小子
普通用户	任何访问者

威胁建模

- 从技术黑盒的角度进行威胁建模
  - 工具、技术、能力发现被攻击面
  - 确定实施渗透的最佳路径
  - 确定控制、流程、架构
- 结果作为渗透测试报告的一部分提交

渗透测试标准 PETS

1. 前期沟通
2. 信息收集
3. 威胁建模
4. 漏洞分析
5. 渗透攻击
6. 后渗透测试
7. 测试报告

漏洞分析

- 漏洞扫描
  - Nessus
  - Openvas
  - Nexpose
  - Nmap script
- 已知漏洞利用
  - Sandi-Gui
  - Searsploit
  - Metasploit
  - Armitage

漏洞分析

- Web 扫描
  - Nikto
  - Burpsuite
  - Owasp ZAP
  - Sqlmap

渗透测试标准 PETS

1. 前期沟通
2. 信息收集
3. 威胁建模
4. 漏洞分析
5. 渗透攻击
6. 后渗透测试
7. 测试报告

渗透攻击

- 未知漏洞挖掘
  - Fuzzing
  - Edb
  - Ollydbg
- 免杀编码绕过
  - Webshell编码和过滤绕过
  - Metasploit
  - Vile-Evasion
- Wifi 渗透
  - Wifite

渗透攻击

- 密码破解
  - Hydra
  - John
  - PTH
  - ccf9155e3e7db453aad3b435b51404ee:3dbde697d71690a769204beb12283678
- 社会工程
  - Metasploit
  - Setools

渗透测试标准 PETS

1. 前期沟通
2. 信息收集
3. 威胁建模
4. 漏洞分析
5. 渗透攻击
6. 后渗透测试
7. 测试报告

后渗透测试

- 扩大战果内网渗透
  - 内网扫描
  - 抓包分析
  - 地址欺骗
- 本地提权
- 获取数据
- 擦除痕迹
- 留后门

渗透测试标准 PETS

1. 前期沟通
2. 信息收集
3. 威胁建模
4. 漏洞分析
5. 渗透攻击
6. 后渗透测试
7. 测试报告

测试报告

- 管理层报告
  - 风险级别
  - 风险分类
  - 整改规划
- 技术报告
  - 漏洞细节
  - 漏洞复现
  - 修补方案

总结

- 安全工作的目标是实现安全
- 渗透测试的目的不是证明系统有多烂，和测试者有多牛
- PETS 是安全实操的方法论，掌握标准但不要迷信标准
- 保持学习状态，重视理论研究，多做上手实践

Thanks !