渗透测试概述

渗透测试流程第5课

360
网络安全学院

教学目标

360 网络安全学院

- 了解渗透测试的基本理念
- 掌握渗透测试的常规流程
- 理解典型的渗透测试案例的思想
- 了解渗透测试与APT之间的关系

360网络安全学院

目录

360网络安全学院

传统渗透测试

传统渗透测试

- 什么是渗透测试
- 为什么要进行渗透测试
- 典型的渗透测试案例

什么是渗透测试

- 问：什么是渗透测试？
- 答：渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。
- 详细描述：渗透测试是指渗透人员在不同的位置（比如从内网、从外网等位置）利用各种手段对某个特定网络进行测试，以期发现和挖掘系统中存在的漏洞，然后输出渗透测试报告，并提交给网络所有者。

什么是渗透测试

360 网络安全学院

- 特点：
  - 1、逐渐深入，常见非web漏洞入口：弱口令、隐私泄露、备份文件泄露等
  - 2、渗透测试不影响正常的业务
  - 3、在进行漏洞测试时一般使用的是已知的漏洞
  - 4、测试完毕后提交安全报告给被测试的一方

360网络安全学院

为什么要渗透测试

- 问：为什么要进行渗透测试？
- 答：
  1、百密一疏，新系统可能存在未知的风险
  2、未雨绸缪，而不是亡羊补牢
  3、专业的渗透测试后，即使是系统未被攻破，也可以以此证明先前实行的防御是有效的
  4、专业的渗透测试可以有效评估系统的安全状况，并提出合理的改进方案

典型渗透测试案例

360 网络安全学院

漏洞概要

缺陷编号：WooYun-[redacted]

漏洞标题：[redacted]内网渗透（一个小问题到最终获取域管理权限）

相关厂商：[redacted]

漏洞作者：路人甲

提交时间：[redacted]

公开时间：[redacted]

漏洞类型：成功的入侵事件

危害等级：高

自评Rank：20

漏洞状态：厂商已经确认

漏洞来源：http://www.wooyun.org，如有疑问或需要帮助请联系 help@wooyun.org

Tags标签：成功入侵

典型渗透测试案例

- 发现弱口令账号（爆破）

➔安全问题：

1、弱口令

2、登陆系统可以爆破

➔可选解决方案：

修改密码、登陆系统、添加验证码

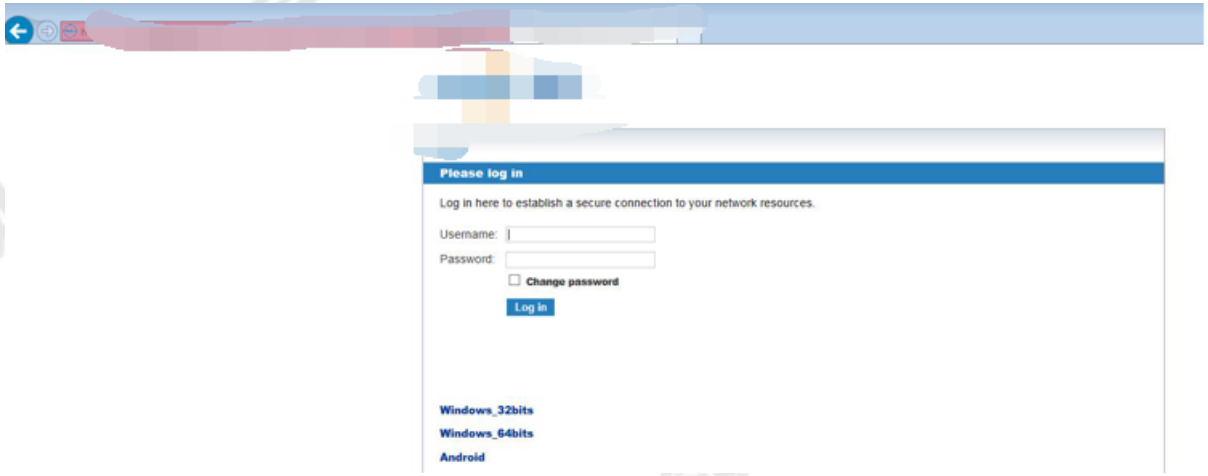
从http://ma[redacted].com/ 爆破出了一枚帐号

luyf:windows@1

典型渗透测试案例

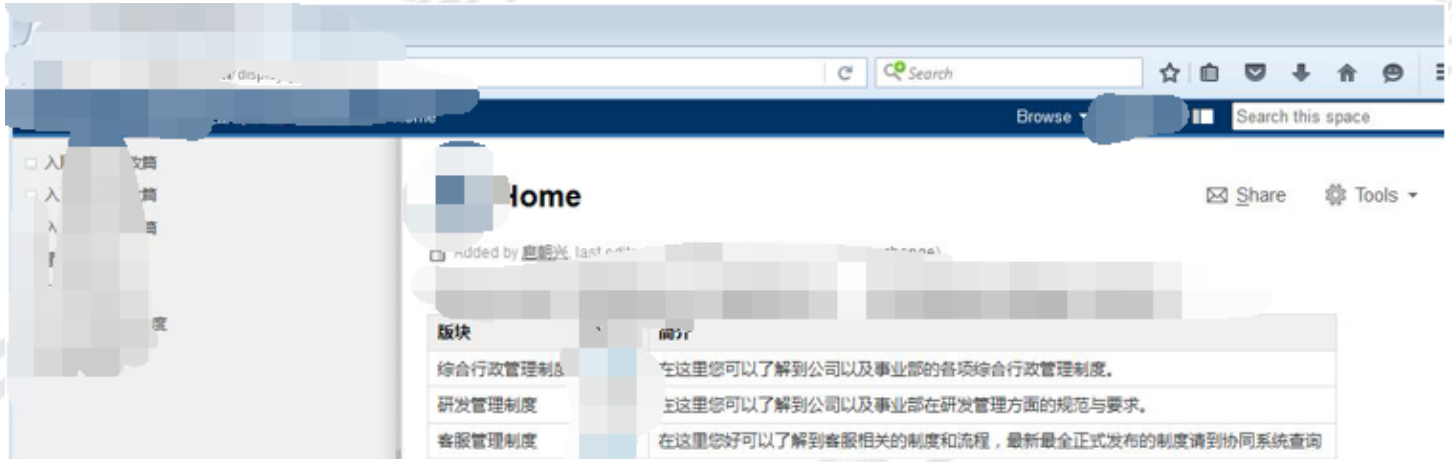
360 网络安全学院

- 发现存在已知漏洞的旧版本vpn软件、
  - ➔安全问题：使用存在漏洞的旧版软件
  - ➔可选解决方案：更新软件



典型渗透测试案例

- 链接vpn进入内网查看内网信息



典型渗透测试案例

360 网络安全学院

- 发现一处命令执行，使用mimikatz获取域管理员账户
  - ➔安全问题：命令执行漏洞
  - ➔可选解决方案：修复漏洞

```
tspkg :
         * Username : backupadmin
         * Domain   : HS
         * Password : *********
        wdigest :
         * Username : backupadmin
         * Domain   : HS
         * Password : ******
```

典型渗透测试案例

360 网络安全学院

- 整体思路：
- 1、Web漏洞——弱口令爆破
- 2、存在漏洞的旧版本软件
- 3、命令执行漏洞

- 最终结果：内网沦陷

360网络安全学院

Apt- 高级持续性威胁

高持续性威胁（apt）

- 什么是apt
- Apt的生命周期
- Apt分析模型
- 典型的apt案例

什么是Apt

360 网络安全学院

- 问：什么是apt？
- 答：利用各种先进的攻击手段，对高价值目标进行的有组织、长期持续性网络攻击行为。
- 详细描述：apt是指攻击者或攻击者组织通过包括0day漏洞、钓鱼等一切手段，在高度隐秘的情况下对目标实施的具有极强目的性的长期控制。

360网络安全学院

什么是Apt

360 网络安全学院

- A——高级（Advanced）
- P——持续（Persistent）
- T——威胁（Threat）

360网络安全学院

什么是Apt

360 网络安全学院

- 特点：

1、高度隐秘

2、高度目的性

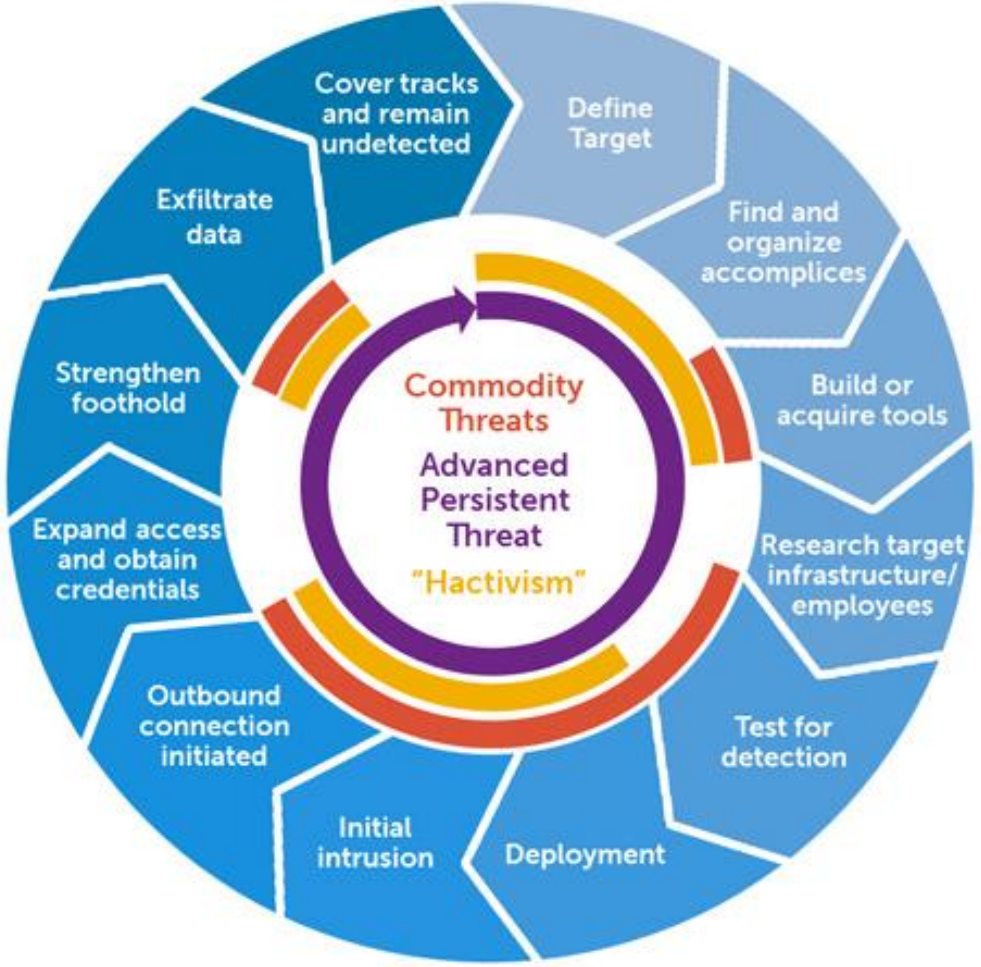
3、手段多样

4、极高的持续性

360网络安全学院

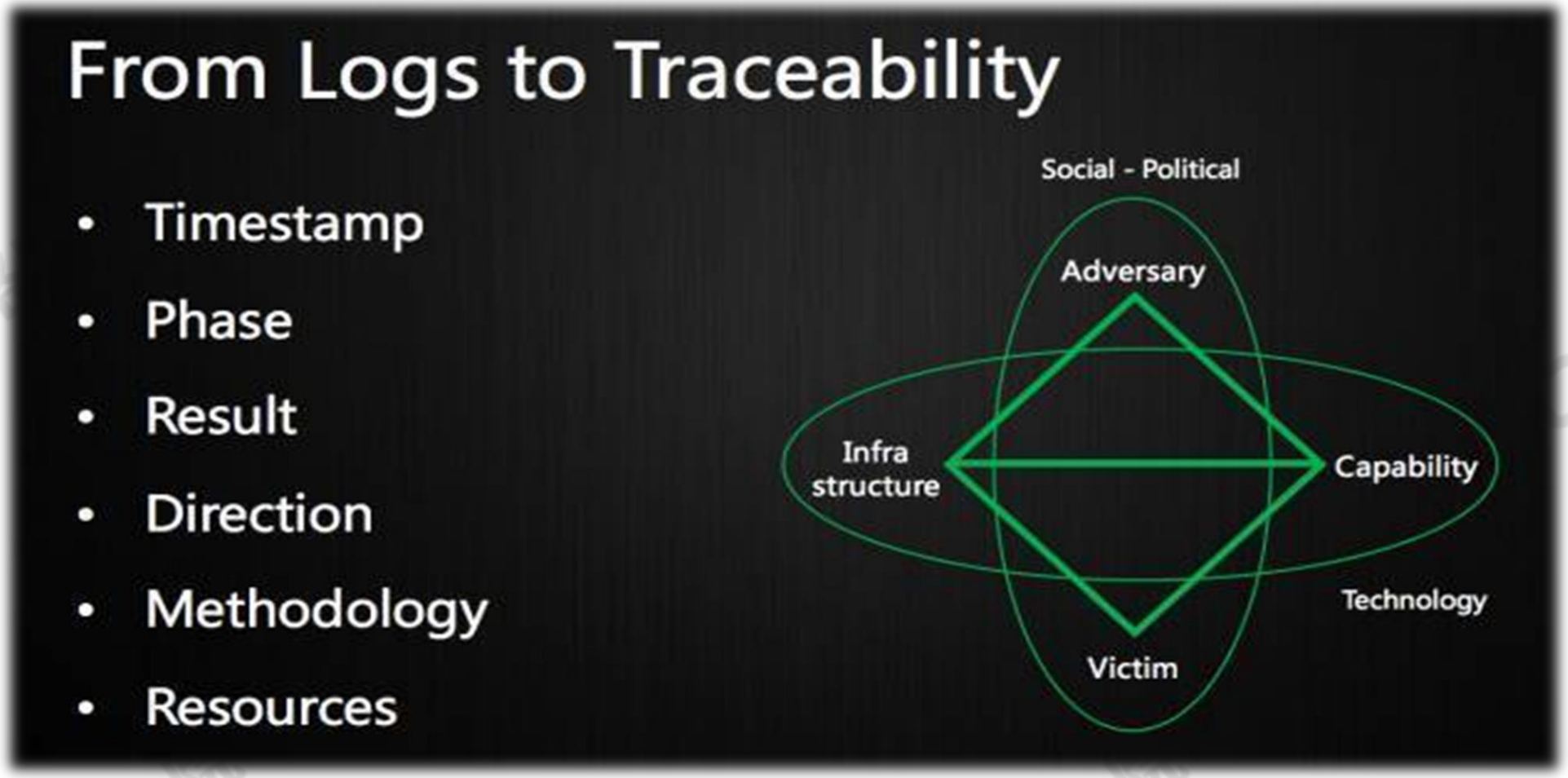
Apt的生命周期

- 从12点方向浅蓝色开始，依次是：
- 1、确定目标
- 2、寻找并建立团队
- 3、建立或取得工具
- 4、调查目标的基础设施或员工信息
- 5、初步测试
- 6、部署完成
- 7、开始攻击
- 8、建立出站链接
- 9、扩大战果并获取凭据
- 10、权限维持并加强控制
- 11、取出数据（达成目标）
- 12、隐藏踪迹并保持未被发现的状态



Apt分析模型-网络杀伤链

Apt分析模型-网络杀伤链



典型的apt案例-RSA SecurID信息被盗事件

360 网络安全学院

- 过程：

  1、向内部人员发送包含攻击载荷（0day）的文件（.xls）

  2、感染一台电脑并植入远控

  3、扩大感染范围

  4、最终进入开发用服务器窃取数据

360网络安全学院

渗透测试与apt的区别

- 目的上：渗透测试的目的是评估计算机网络系统的安全性；而apt的目的是对高价值目标进行的有组织、长期持续性的控制。
- 手段方法上：渗透测试通过被允许的行为模拟黑客攻击来对目标系统进行测试；而apt利用任何各种高技术手段（包括0day漏洞、欺骗性的钓鱼邮件等）进行攻击。
- 结果上：渗透测试提高了目标系统的安全级别；而apt在达成目的的过程中一般会给目标系统带来严重损失。

总结

- 重点知识

渗透测试、APT的基本流程

- 难点知识

渗透测试过程中的技术应用

360网络安全学院

谢谢

360
网络安全学院