

期末复习知识点

第一章 概论

1. 网络空间安全的定义

- ◆ 网络空间安全要素模型★★
- ◆ Safety 与 Security 的辨识★★
- ◆ 网络空间安全的威胁类型★
- ◆ 网络空间安全目标★
- ◆ 密码学、系统安全和网络安全之间的关系★★

2. 网络空间安全的科学性

- ◆ 科学的目标
- ◆ 归纳域与演绎域的概念及辨析★★★
- ◆ 网络空间安全科学中的归纳域/演绎域裂痕★★★
- ◆ 定性结论与定量结论★★

3. CSEC2017 课程框架

- ◆ CSEC2017 的知识域
- ◆ CSEC2017 的网络空间安全知识框架

4. 小结

- ◆ 网络空间安全要素模型
- ◆ 网络空间安全目标
- ◆ 系统思维与对手思维★★

第二章 网络攻击

5. 网络攻击的基本概念

- ◆ 攻击的发起★
- ◆ 攻击的目的★
- ◆ 攻击的形式★
- ◆ 攻击的进化★★
- ◆ 黑客的类型★★

6. 安全漏洞

- ◆ 漏洞的概念★★
- ◆ 漏洞的披露★★★
- ◆ 漏洞的生命周期★★★
- ◆ 设计漏洞\实现漏洞\管理漏洞的理解与辨析★★

7. 漏洞库

- ◆ CVE★★
- ◆ CWE\CPE★
- ◆ NVD & CNNVD★
- ◆ Exploit-DB

8. 入侵攻击模型

- ◆ 入侵攻击的传统模式★
- ◆ 网络杀伤链★★★★
- ◆ ATT&CK 模型★★

9. 进入方法

- ◆ 进入的目的★
- ◆ 主动进入与被动进入的概念、辨析与举例★★★★

10. 提权方法

- ◆ 提权的目的★
- ◆ 特权程序漏洞利用的例子★
- ◆ 路径/配置劫持★
- ◆ 配置不当利用的例子★

11. 木马后门

- ◆ 木马程序★
- ◆ 木马后门★★
- ◆ 木马的类型★★

12. 服务失效攻击

- ◆ 攻击目的★
- ◆ DoS 的攻击机制★★
- ◆ DDoS 攻击的对象★
- ◆ DDoS 攻击的直接放大机制★★
- ◆ DDoS 攻击的反射放大机制★★★★
- ◆ 面向 BGP 协议的跨平面协同会话阻断攻击

13. 小结

- ◆ 基本概念：攻击、故障、事故的区别，黑客的种类，漏洞的种类；
- ◆ 对网络攻击的宏观理解：传统攻击模型，网络杀伤链，ATT&CK 模型（技术、战术、过程）；
- ◆ 对网络攻击的微观理解：如何利用设计漏洞、实现漏洞、管理漏洞实施攻击；进入攻击，提权攻击，木马后门（滞留攻击），服务失效攻击。

第三章 僵尸网络

1. 网络蠕虫

- ◆ 潜代码\恶意软件\恶意代码★
- ◆ 网络蠕虫概念的出现
- ◆ Morris 蠕虫（事件过程、基本工作机制、存活机制、功能特征）★★★
- ◆ 网络蠕虫的传播机制★★
- ◆ 蠕虫的进化★
- ◆ 蠕虫的功能构成★★
- ◆ 蠕虫的典型代码结构★
- ◆ 蠕虫代码的加壳与脱壳

2. 僵尸网络

- ◆ Zombie 的概念★
- ◆ Zombie 的工作流程★★★
- ◆ 僵尸网络的生命周期模型★★
- ◆ 僵尸网络具有三个基本行为★★
- ◆ 僵尸网络发展简史★
- ◆ 僵尸网络的基本控制结构★★★
- ◆ 僵尸程序控制结构代码示例
- ◆ 僵尸网络的生存机制★★
- ◆ 检测逃逸的概念★
- ◆ FFSN 的概念★
- ◆ 切换机制：IP fluxing 机制等★★★

3. 小结

- ◆ Morris 蠕虫使用的攻击机制和攻击流程
- ◆ 网络蠕虫的基本功能及其目的
- ◆ 僵尸网络的构成
- ◆ 僵尸网络的生命周期模型
- ◆ Fast Fluxing 机制★★★

第四章 黑产

1. 基本方法

- ◆ 黑色产业链的定义★
- ◆ 对内：基于合作和暗网/对外：基于社会工程方法★
- ◆ 黑产的分工合作★★
- ◆ 暗网的定义、特点、例子★★★
- ◆ 社会工程攻击及相关概念（社会工程学，社会工程攻击者，社会工程方法，社会工程攻击）★★★
- ◆ 社会工程攻击的本体论模型★★
- ◆ 社会工程攻击流程★★★
- ◆ 社会工程攻击的物理手段与心理手段★★
- ◆ 网络钓鱼攻击★
- ◆ 基于社会工程的网络钓鱼★★
- ◆ 基于技术手段的网络钓鱼★★

- ◆ 鱼叉攻击★★
 - ◆ 网络钓鱼的基本攻击方法（访问欺骗\恶意代码注入信息注入）★★★
2. 面向下载的黑色产业链
 - ◆ PPI 模式★★
 - ◆ 基于流量的 PPI★
 3. 面向销售的黑色产业链
 - ◆ 基本构成（广告发布，点击支持，销售实现）★★
 - ◆ 实例：盗版药品销售。
 4. 恶意的黑色产业链
 - ◆ 隐私信息盗取（撞库、拖库、洗库）★★★★
 - ◆ 勒索软件的定义★★
 - ◆ 勒索软件的基本工作机制★★★★
 - ◆ 用户域解密机制与攻击者域解密机制★★★★
 - ◆ APT 攻击★★
 - ◆ APT 攻击形式★★★★
 - ◆ 震网行动
 - ◆ 奇幻熊
 5. 小结
 - ◆ 通过社会工程攻击的本体论模型了解基本概念
 - ◆ 通过社会工程攻击框架了解攻击链构成
 - ◆ 黑产的合作模型与角色分工
 - ◆ 黑产的类型

第五章 滥用入侵检测

1. 基本概念
 - ◆ 网络监测\网络安全监测\网络内容监测★
 - ◆ 网络安全监测系统★★
 - ◆ 监测点(NIDS\HIDS)★★
 - ◆ 监测手段（漏洞扫描系统\蜜罐系统\警报系统\网络管理系统）★★
2. 入侵检测系统
 - ◆ 入侵检测系统的定义★
 - ◆ 入侵检测系统的功能★
 - ◆ 网络入侵检测的基本模型★★★★
 - ◆ 检测精度(误报，漏报，基率谬误，准确率)★★
 - ◆ 基率谬误（base-rate fallacy）
3. 网络异常检测的基本概念
 - ◆ 异常行为的概念★

- ◆ 网络异常检测★★
- ◆ 异常检测的通用框架★★

4. 网络滥用检测

- ◆ 网络滥用检测的概念★★
- ◆ 滥用检测基本架构★★
- ◆ 数据采集方法★
- ◆ 数据的物理采集形式★
- ◆ 数据采集流程（2-Copy\Zero-Cop\DPDK）★★
- ◆ 数据采集工具(PCAP\TCPDUMP\Wireshark)★★
- ◆ 检测规则★
- ◆ Snort 的检测规则★★
- ◆ Snort 规则结构与实例★
- ◆ Zeek 的检测规则★
- ◆ Zeek 规则结构与举例；

5. 规则匹配

- ◆ 报文分类的概念★
- ◆ 报文分类算法的性能测度★★
- ◆ HiCuts 算法-几何空间分割法★
- ◆ BM 算法(Boyer-Moore algorithm)★

6. 事件后处理

- ◆ 冗余消除★★
- ◆ 基于相似性的关联判定★★
- ◆ 警报融合★
- ◆ 基于因果关系的关联判定★

7. 开源系统介绍

- ◆ Snort 系统架构\Suricata 系统架构\Zeek 系统架构★
- ◆ Suricata 系统检测日志举例；
- ◆ Zeek 系统检测日志举例。

8. 蜜罐系统介绍

- ◆ 蜜罐的定义★
- ◆ 蜜罐的分类★★

9. 蜜罐的部署

- ◆ 蜜罐的实现(低交互蜜罐\高交互蜜罐)★★
- ◆ 蜜罐的核心机制★★
- ◆ 蜜罐的辅助机制★
- ◆ 蜜网系统★★
- ◆ 蜜场的概念★★

10. 小结

- ◆ 系统架构：网络滥用入侵检测模型；检测结果的准确性

- ◆ 数据采集：报文采集的零拷贝技术；PCAP 格式
- ◆ 检测规则：高维分类与 HiCuts 算法、BM 算法
- ◆ 事件后处理：冗余消除、误报消除、事件融合
- ◆ 蜜罐：基本工作原理、系统结构、蜜罐类型

第六章 网络安全防御

1. 网络安全管理

- ◆ 系统的可生存性★★
- ◆ 入侵防御\入侵检测\入侵容忍的辨析★★★
- ◆ 系统的可生存性要素★
- ◆ 网络的纵深防御概念★★★
- ◆ 网络安全管理的必要性（原因）★
- ◆ 网络防御原则★
- ◆ 网络安全管理的工程要求★
- ◆ 网络安全管理的基本任务★
- ◆ 网络安全管理的实现★

2. 脆弱性评估

- ◆ 漏洞扫描的概念★
- ◆ 基于 TCP 的端口扫描★★★
- ◆ UDP ICMP 端口扫描★★★
- ◆ 扫描对象选择（遍历性扫描\选择性扫描）★★
- ◆ 扫描方式（显式扫描\隐式扫描）★★
- ◆ 扫描工具 NMAP★★
- ◆ 扫描工具 ZMAP★★
- ◆ ZMAP 与 NMAP 的比较★★★
- ◆ 攻击图★
- ◆ 基于攻击图的脆弱性评估方法（对象建模、攻击图构造）★

3. 协同防御

- ◆ 协同防御的概念★★
- ◆ 入侵检测组件协同场景★
- ◆ 入侵协同阻断系统★
- ◆ 基于 GrIDS 的协同防御举例
- ◆ CITRA 的系统架构★

4. 威胁情报交换标准

- ◆ 网络空间的威胁情报的概念★
- ◆ 内部情报与外部情报★★
- ◆ 可机读威胁情报与人读情报★★
- ◆ 威胁情报种类（行动级\战术级\战略级）★
- ◆ 制定威胁情报交换标准的目的★★
- ◆ STIX（对象类型、匹配模式）★

5. 应急响应

- ◆ 安全事件的概念★
- ◆ 安全事件应急响应★
- ◆ 安全事件类型★
- ◆ 网络安全事件的响应策略（封堵方式，捕捉方式）★★
- ◆ 应急响应处理流程框架★★

6. 小结

- ◆ 网络安全管理：系统的可生存性概念；网络安全的纵深防御概念；网络安全管理的工程要求；
- ◆ 脆弱性评估：端口显式扫描和隐式扫描的工作原理；NMAP 的工作原理；ZMAP 的工作原理；攻击图分析方法的基本原理；
- ◆ 协同防御：入侵检测组件的协作场景；威胁情报的基本概念-内部情报、外部情报、结构化情报、无结构情报；IoC 的概念；STIX 的应用场景；
- ◆ 应急响应：安全事件类型；响应策略；处理流程。

第七章 网络攻击阻断

1. 防火墙

- ◆ 防火墙的概念★
- ◆ 防火墙的基本架构★★
- ◆ 防火墙的类型★★
- ◆ 防火墙的实现方式★★
- ◆ IP 级防火墙★★★
- ◆ 内向流量\外向流量\内向服务\外向服务★★★
- ◆ 规则处理★★
- ◆ Linux 防火墙（Netfilter + Iptables）★★
- ◆ 状态检测的概念★
- ◆ 状态检测防火墙★★
- ◆ DPI（报文深度检测）★
- ◆ 防火墙的使用（有孔过滤方式、堡垒主机方式、DMZ 方式、网关方式）★★★

2. 会话拦截

- ◆ TCP 拦截阻断★★
- ◆ DNS 重定向阻断★★★
- ◆ DNS 缓存污染★★

3. 数字取证

- ◆ 计算机取证的概念★
- ◆ 基本过程模型★
- ◆ 集成数字取证过程模型 IDFPM
- ◆ 操作原则★★
- ◆ 技术分类★

- ◆ 使用环境分类（互联网取证、物联网取证、云环境取证、移动设备取证）★
- ◆ 操作流程★★

4. 黑色郁金香★★★

- ◆ DigiNotar 公司的基本情况★
- ◆ 攻击事件的发现过程★★
- ◆ 事件响应过程★★
- ◆ 数字取证调查过程★★★
- ◆ 陈述决策过程★

5. 小结

- ◆ 防火墙：IP 防火墙、应用防火墙和 WAF 的工作原理；过滤策略的定义；防火墙的部署方式。
- ◆ DNS 拦截：重定向；缓存污染。
- ◆ 数字取证：基本过程模型；IDFPM 模型；基本操作流程。

第八章 网络安全访问

1. 鉴别

- ◆ 认证与鉴别的概念辨析★★
- ◆ 鉴别的作用★
- ◆ 鉴别的凭证★
- ◆ 零知识证明的概念★★
- ◆ 单向鉴别（基于共享秘密的单向鉴别、基于非对称密钥的单向鉴别）★★★
- ◆ 双向鉴别（基于共享密钥，基于非对称密钥）★★★
- ◆ 消息鉴别码 MAC（传输数据的完整性鉴别机制、HMAC 及其实现方式）★

2. 口令

- ◆ 口令的基本概念★
- ◆ 口令技术的优点★★
- ◆ 口令技术的脆弱性★★★
- ◆ 口令管理方式（拆分方法、一次一密方法、变换方法、KDC 方法）★★★
- ◆ 口令攻击（在线猜测、字典攻击）★★
- ◆ 多重口令机制★
- ◆ 口令恢复机制的基本要求★★
- ◆ 基于知识的口令恢复机制★★
- ◆ 基于安全通道的口令恢复机制★★

3. KDC

- ◆ SSO 的概念（一次鉴别多次使用）★★★
- ◆ 可信中继模型★★
- ◆ Needham-Schroeder Scheme 与增强的 Needham-Schroeder Scheme★★★
- ◆ KEBEROS 的基本知识（起源，基本模型，现有版本）★

- ◆ KEBEROS 基本术语（主体，客体，鉴别服务器，TGT）★★★
- ◆ KEBEROS 基本工作流程（TGT 的获得、端系统访问的鉴别过程）★★★
- ◆ KEBEROSV4 系统的跨域鉴别★★
- ◆ KEBEROSV5 系统的代理概念★★
- ◆ V5 系统的跨域鉴别（信任链方法）★★
- ◆ TLS 与 SSL★★

4. 身份管理

- ◆ 鉴别中的身份信息管理问题（最小信息披露问题等）★★
- ◆ 身份管理的基本概念（IdP, SP 等）★★
- ◆ 身份管理的基本工作流程★★
- ◆ Shibboleth 的基本知识★

5. 匿名通信

- ◆ 匿名通信的基本概念★★
- ◆ 广播方法★
- ◆ 匿名链方法★★
- ◆ 洋葱路由方法（Tor）★★★

6. 小结

- ◆ 鉴别：鉴别的作用；零知识证明；HMAC；口令管理方法；Needham-Schroeder 模型；KEBEROS 系统的工作原理；KERBOROS 的跨域鉴别和代理鉴别方法。
- ◆ 身份管理：基于 IdP 的身份鉴别与授权处理流程。
- ◆ 匿名通信：匿名通信的需求；DC-net 方法，匿名链方法，洋葱路由方法。

第九章 网络基础设施保护

1. 链路层保护

- ◆ 安全的依赖性★
- ◆ 链路层面临的安全威胁★★
- ◆ 常用保护机制（端口安全、DHCP 窥探、动态 ARP 检测、IP 源保护）★★
- ◆ AAA 的概念★
- ◆ RADIUS 服务器

2. 802.1X

- ◆ 基本原理★
- ◆ 基本架构★
- ◆ 基于 MD5-Challenge 的 EAP 中继方式认证过程★
- ◆ 基于 CHAP 的 EAP 终结方式认证过程★

3. IPv4 和 IPv6 的安全问题

- ◆ 缺乏鉴别功能（假冒源地址、服务抢占、服务失效）★★
- ◆ 机制可以被滥用（恶意竞争、意使用报头字段或选项功能）★★
- ◆ 不恰当的设计★★
- ◆ 实现的不一致性★
- ◆ IPv4 报头存在的问题★★
- ◆ IPv4 协议机制中的安全漏洞★★★
- ◆ IPv6 报头格式及其改进★★
- ◆ IPv6 协议机制中的安全漏洞★★

4. IPsec

- ◆ IPsec 基本知识（基本格式、实现方式、使用模式）★★★★
- ◆ IPsec 系统架构（SPD、SAD、PAD）★★★★
- ◆ 报文处理流程（离去报文处理流程；到达报文处理流程）★★
- ◆ ESP（报头格式；负载格式）★
- ◆ AH（报头格式；负载格式）★
- ◆ IKE 的报文类型★★
- ◆ IKE 的基本工作流程★★

5. DNSSEC

- ◆ DNS 基本概念★
- ◆ DNS 报文格式★
- ◆ DNS 解析过程★
- ◆ DNS 的安全威胁★★
- ◆ DNSSEC 基本概念★★
- ◆ DNSSEC 新增的资源记录★★
- ◆ DNSSEC 的信任链（鉴别密钥，签名密钥 KSK，ZSK）★★★★
- ◆ DNSSEC 的使用（DNSSEC 解析过程举例）★★★★
- ◆ DNSSEC 的部署★★

6. 小结

- ◆ 链路层保护：端口绑定和协议窥探的概念；RADIUS 和 802.1x 的工作原理；
- ◆ IP 安全：ESP 和 AH 的功能和保护范围；传输模式和隧道模式的概念；SA 的概念；SPD、SAD 和 PAD 等三个数据库的作用；IPsec 的报文处理流程；IKE 协议的工作原理。
- ◆ DNS 安全：RRSIG、DNSKEY、DS 和 NSEC 等资源记录的作用；DNSSEC 的工作流程；DNSSEC 的密钥管理方法。