清华大学本科生考试试题专用纸

考试课程 网络空间安全导论 （A卷） 2022年06月12日

一、不定项选择（共17题，每题2分）

（1）基于异常检测的IDS，相比于基于固定规则的IDS，最显著的优点是：（）

A. 误报率低

B. 可以识别未知攻击

C. 检测速度快

D. 计算开销低

（2）链路层常见的攻击有：（）

A. Wi-Fi 帧嗅探

B. ARP 污染

C. IP 分片误用

D. SYN Flooding 攻击

（3）传输层安全性协议（TLS）提供的安全功能包含了：（）

A. 数据加密

B. 身份认证

C. 数据完整性验证

D. 身份与公钥绑定

（4）针对SYN Flooding攻击，以下哪些属于内核层防御：（）

A. MAC-IP Bindings

B. ARP Reply Discarding

C. SYN Filtering

D. SYN Cookie

（5）以下属于DNSSEC使用的资源记录类型的是：（）

A. DNS 公钥

B. 委托签名

C. 公钥基础设施

D. 资源记录签名

（6）下列操作系统内存防御机制当中，需要借助硬件实现的是：（）

A. ASLR

B. W^X

C. SMAP

D. Stack Canary

（7）OpenSSL 的心脏滴血漏洞（Heartbleed Attack），属于下列哪一种堆区安全漏洞？（）

A. Use-After-Free

B. Heap Over-read

C. Double-Free

D. Heap Overflow

（8）进程的控制流完整性保护（CFI）运行前需要获得程序的：（）

A. 抽象语法树（Abstract Syntax Tree，AST）

B. 控制流图

C. 数据流图

D. 程序依赖图

（9）地址空间布局随机化 (ASLR)随机化哪些内存段基地址：（）

A. 代码段

B. 栈区

C. 堆区

D. 内存映射段

（10）在 CPU 缓存侧信道攻击中需要不断探测目标数据是否被 CPU 缓存，以下哪些 CPU 缓存侧信道攻击方法在探测时无需内存读取即可判断目标数据是否被缓存：（）

A. Evict-Reload

B. Prime-Probe

C. Flush-Flush

D. Flush-Reload

（11）以下哪些措施可以缓解骑士攻击：（）

A. 限制固定的电压/频率对

B. 禁止处理器超频

C. 验证电压管理驱动的完整性

D. 禁用处理器电压的模式寄存器

（12）面向机器学习算法的攻击方案中，假设攻击者无法获知机器学习所使用的具体算法，以及算法所使用的参数的攻击方案可以被定义为：（）

A. 有目标攻击

B. 无目标攻击

C. 白盒攻击

D. 黑盒攻击

（13）分布式系统当中，某一节点的全体邻居由攻击者控制的恶意节点组成的现象被称为：（）

A. 节点故障

B. 日蚀攻击

C. 拜占庭节点攻击

D. 女巫攻击

（14）以下关于差分隐私的描述，正确的是：（）

A. 差分隐私方法可以提高数据的可用性

B. 差分隐私中加入噪声太少会降低安全性，所以噪声越多越好

C. 差分隐私可以保护个体数据

D. 差分隐私主要分为数值型和非数值型（离散型）

（15）请选出下列算法中的半同态加密算法：（）

A. Gentry

B. BGV

C. Paillier

D. GSW

（16）以下关于散列函数的说法正确的是：（）

A. 合格的散列函数应具有单向性与一定的抗碰撞性

B. 散列函数算法 SHA-3 可以生成任意长度的摘要

C. 由于其单向性，散列函数不能参与数字签名过程

D. MD5 的强碰撞性已被攻破，但 SHA 系列所有算法仍未被攻破

（17）以下关于加密算法的说法中，**错误**的是：（）

A. 对称加密算法在密钥分发过程中被窃听可能导致安全问题，但公钥加密算法不会。

B. 全同态加密算法十分强大，整体性能也要优于半同态算法。

C. 理论上来说，没有任何一种加密算法是绝对安全的，甚至暴力破解也是有可能成功的。

D. 公钥密码技术不仅可以用来加密解密，也可进行身份验证，这是对称加密做不到的。

二、填空（共 13 题，每空 1 分）

（1）攻击者伪装成受害主机，广播大量的 ping 请求(ping flooding)，是一种基于_ICMP__协议的 DDoS 攻击。

（2）IPSec 协议与 SSL 协议分别保护_网络_层、__传输__层的数据。

（3）常见的 IPID 分配算法主要包括_基于全局计数器的 IPID 分配__、__基于哈希值的 IPID 分配_、随机 IPID 分配、单目标以及单连接 IPID 分配。

（4）相较于本地缓存中毒攻击，DNS 远程缓存中毒攻击加大了_16 位 UDP 源端口号_、__16 位的事务 ID 号_____两个数据的获取难度。

（5）DNSSEC 基于 DNS 区域层次结构提供信任链，DoT 和 DoH 均以_PKI_为信任基础。

（6）针对机器学习算法的投毒攻击将恶意样本混入_训练数据中_实现对模型的修改。

（7）攻击者利用同一堆块被释放两次的错误编码逻辑构造的堆区攻击被称为_Double-Free_。

（8）Stack Canary 防御栈溢出的原理是：在栈帧中保存的_EBP_寄存器数值之后插入随机性内容。

（9）全局偏置表劫持攻击（GOT Hijacking）当中的受害全局偏置表位于_数据_段。

（10）故障注入攻击的主要方式有_电压故障注入_、_频率故障注入__、_电磁攻击_____。

（11）中央处理器的安全模型一般可以分为_特权级模型_和_隔离模型_。

（12）同态加密方案一般包含_KetGen_、_Encrypt_、_Decrypt_、_Evaluate_四个算法，其中的_ Evaluate _算法是同态加密的核心。

（13）在数据隐私保护技术中，_匿名化_技术可以隐藏用户身份和数据的对应关系，_差分隐私_技术可以隐藏真实数据、只呈现出数据的统计学特征，_同态加密_技术则可以使数据对非拥有者不可见。

三、问答（共 5 题，前 4 题每题 8 分，第 5 题 9 分）

（1）请描述 off-path 类型的攻击者在劫持一个目标 TCP 连接时，需要具备哪些能力？攻击者在注入伪造的报文时，需要猜测出 TCP header 里面的哪些字段，原因是什么？

书 p268 280

攻击者可以伪装身份，攻击者需要推理猜出 TCP 连接的状态信息

攻击者需要猜出连接的源端口号，序列号和应答号

（2）请解释并对比针对机器学习算法的逃逸攻击和后门攻击。

（3）简要描述 Meltdown 与 Spectre 的攻击原理，并比较其共同点和区别。

第五讲 ppt p57

第五讲 ppt p60

（4）简述常见的各类跨站点脚本攻击 (XSS) 和跨站请求伪造攻击（CSFR) 的原理和攻击流程。

第 12 讲 ppt p12 p14

（5）请简述以下三种常见的内存防御机制的原理：

a. W^X (Write XOR eXecution)

b. ASLR (Address Space Layout Randomization)

c. Stack Canary

并讨论这三种防御机制在阻碍攻击者设计并实施面向返回地址编程 (ROP) 时能否起到作用。