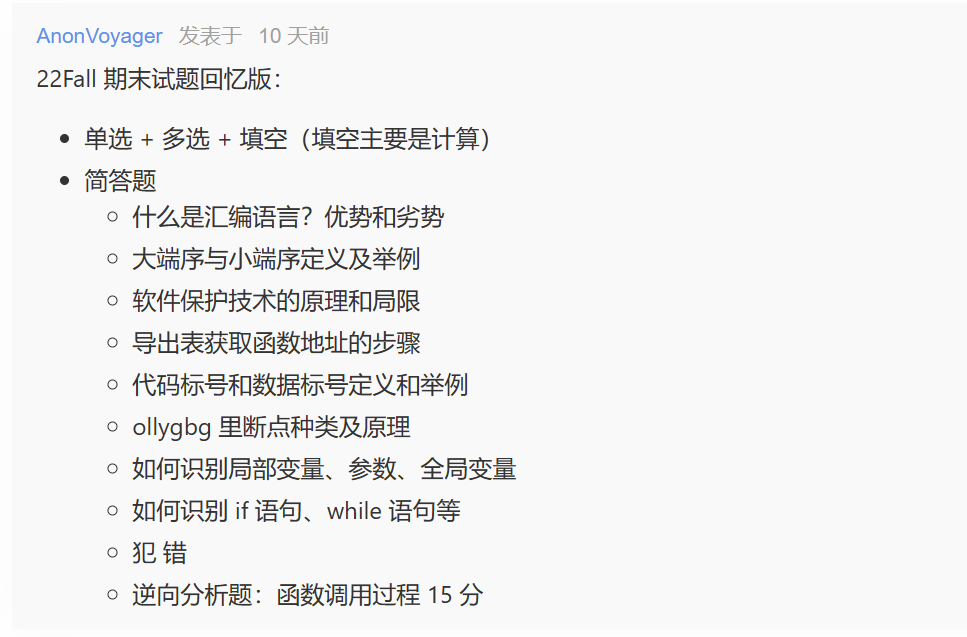
单选10

不定项5

填空5

简答

逆向分析1



**第二章**

十六进制数据表示（h后端，字母前面加0）

字符集（用二进制来表示不同的字符）

字节序（大端小端）

**第三章**

寄存器（eax,ecx）

IA-32位处理器体系结构（保护模式？独立的4GB空间，EFLAGS寄存器）

内存管理（段&页模式，一页4096字节内存块，存1024个项）

**第四章**

标识符（data，code）

指令&伪指令

数据定义（byte：1，word：2，dword：4，dup：很大的数据空间）

符号常量

**第五章**

控制流转移（CMP,LOOP-ecx,条件跳转）

过程的定义（PROC,ENDP,CALL,RET，前两个伪指令，后两个指令）

调用库函数（PROTO伪指令）

**第六章**

数据传送

加减法

数据伪指令

间接寻址——相对基址变址

**第七章**

ARM寻址方式

ARM8的架构的体系结构

指令集、伪指令（寄存器-内存，内存-寄存器，简单的）

语言程序结构（helloworld）

编译与调试工具（helloworld程序）

**第八章**

可执行文件

虚拟地址（VA）、相对虚拟地址（RVA）

DOS文件头（向下兼容）MZ-4D5A

PE文件头

**第九章**

节表

导入表

导出表

**第十章**

不会考察**工具**的使用

简介、窗口、操作不考

知识点都要复习

增强反汇编？

**第十一章**

不考核工具的使用

基本概念？什么是动态逆向分析

Memory map

执行指令

Breakpoint（怎么实现软件断点？CC指令）（硬件断点？不修改指令，内部有个寄存器，记录的内存地址被执行就会产生中断）（内存的断点，内存属性的中断）。。。

**第十二章**

识别函数——**参数、局部变量（栈指针减去空间）、栈指针、函数调用约定（从右向左，传递到栈上）**

**第十三章**

序列号保护（脆弱性？）

警告窗口

时间限制

菜单功能限制

Keyfile保护（可以很长）

**考点：**

**第二章**

汇编语言的概念，优点与缺点

汇编语言的应用场景

数据的存储单位

字节序的两种方式，举例说明

**第三章**

CPU的基本结构

执行一条机器指令的一系列操作

IA-32位处理器的两种工作模式

通用寄存器（8种）

EFLAGS寄存器的使用

段寄存器的构成

分页机制

从虚拟地址中读取一个内存数据，怎么访问内存？

**第四章**

汇编语言的基本元素（10种）

数据标号与代码标号

DUP伪指令的使用

**第五章**

控制流转移的两个方式

各种条件跳转的名字以及含义

LOOP的操作方式（ECX）

过程，启动过程

PROTO伪指令

**第六章**

操作数的类型（立即数、寄存器、内存…）

EAX,AX,AH,AL

内存操作数

MOVZX与MOVSX

LAHF,SAHF

XCHG

直接偏移操作数

INC,DEC,ADD,SUB,NEG

OFFSET

ALIGN

PTR

TYPE

LENGTHOF

SIZEOF

LABEL

间接寻址——一维数组的访问

几种寻址的方法

TYPEDEF

**第七章**

ARMv8的两种架构——AArch32,AArch64

分别的寄存器的数量与位数，指令集使用

ARM的寻址方式

LDR,STR,SWP

ARM的基址寻址的三种方法

IA,IB,DA,DB

FD,FA,ED,EA

ARM指令集

**第八章**

Windows可执行文件的格式

PE文件的结构

RVA与VA的关系

DOS文件头

**第九章**

节表记录的信息

块属性——前两位（可执行，可读，可写）

节的内容属性——后两位（可执行，已初始化，未初始化）

RVA与RAW的转化

导入表的获取函数地址的操作

导出表的获取函数地址的操作

**第十章**

增强反汇编的功能

函数名、局部变量、参数的前缀、后缀、偏移

**第十一章**

反汇编窗口

相对地址、绝对地址

断点的分类与优缺点

**第十二章**

ESP,EBP,PUSH,POP

RETN指令

调用约定

如何识别变量、数组、结构体

如何识别if、switch、for、while、do while分支结构

**第十三章**

软件保护技术的方式以及缺陷？