

山东省第一届职业技能大赛网络安全项目

模块 B

网络安全事件响应、数字取证调查和应用程序安全

赛题

目录

目录.....	1
模块 B 竞赛项目样题.....	2
介绍.....	2
所需的设备和材料.....	2
评分方案.....	2
项目和任务的描述.....	2
工作任务.....	3
第一部分 网络安全事件响应.....	3
任务 1: 应急响应.....	3
本任务素材清单: WebServer 服务器虚拟机 (Linux 或 Windows 操作系统)	3
第二部分 数字取证调查.....	3
任务 2 : 操作系统取证.....	3
本任务素材清单: 内存镜像 (*.vmem)、存储镜像 (*.img 等)	4
任务 3: 网络数据包分析取证.....	4
本任务素材清单: 捕获的网络数据包文件 (*.pcapng、*.pcap 等)	4
任务 4: 计算机单机取证.....	4
本任务素材清单: 取证镜像文件 (*.e01、*.img 等)	5
第三部分 应用程序安全.....	5
任务 5: 应用程序安全分析.....	5
本任务素材清单: 应用程序文件 (ELF、*.exe、*.sys 等)	5
任务 6: 代码审计.....	6
本任务素材清单: 源代码片段 (php、python、c、java 等)	6
分值分配表.....	7

模块 B 竞赛项目样题

本文件为：山东省第一届职业技能大赛网络安全项目试题-模块 B 样题

本次比赛时间为 5 个小时。

介绍

竞赛有固定的开始和结束时间，参赛队伍必须决定如何有效的分配时间。请认真阅读以下指引！

- (1) 当竞赛结束，离开时请不要关机；
- (2) 所有配置应当在重启后有效；
- (3) 请不要修改实体机的配置和虚拟机本身的硬件设置。

所需的设备和材料

所有测试项目都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

评分方案

根据目前技术描述中的技能大赛标准规范，这个测试项目模块分数为 50 分。

项目和任务的描述

随着网络和信息化水平的不断发展，网络安全事件也层出不穷，网络恶意代码传播、信息窃取、信息篡改、远程控制等各种网络攻击行为已严重威胁到信息系统的机密性、完整性和可用性。因此，对抗网络攻击，组织安全事件应急响应，采集电子证据等技术工作是网络安全防护的重要部分。现在，A 集团已遭受来自不明组织的非法恶意攻击，您的团队需要帮助 A 集团追踪此网络攻击来源，分析恶意攻击攻击行为的证据线索，找出操作系统和应用程序中的漏洞或者恶意代码，帮助其巩固网络安全防线。

任务分为以下几个部分：

- 网络安全事件响应
- 数字取证调查
- 应用程序安全

本部分的各任务试题素材已放置在选手操作机对应任务目录下，参赛选手完成任务后，请将答案填写在电脑桌面上“山东省第一届职业技能大赛网络安全项目-模块 B 答题卷”中。

选手的电脑中已提供了竞赛所需的软件。

工作任务

第一部分 网络安全事件响应

任务 1：应急响应

A 集团的 WebServer 服务器被黑客入侵，该服务器的 Web 应用系统被上传恶意软件，系统文件被恶意软件破坏，您的团队需要帮助该公司追踪此网络攻击的来源，在服务器上进行全面的检查，包括日志信息、进程信息、系统文件、恶意文件等，从而分析黑客的攻击行为，和残留的关键证据信息。

本任务素材清单：WebServer 服务器虚拟机（Linux 或 Windows 操作系统）

受攻击的 WebServer 服务器已打包成 VMWare 虚拟机，请选手启动虚拟机进入操作系统进行分析。

操作系统登录用户名/密码：root/123456

请按答题卡的要求完成该部分的工作任务。

任务 1：应急响应		
序号	任务要求	答案
1	请提交攻击者的 IP 地址	
2	请写出攻击者使用的操作系统	
3	请提交攻击者写入的木马文件名称	
4	

第二部分 数字取证调查

任务 2：操作系统取证

A 集团某电脑系统被恶意份子攻击并控制，怀疑其执行了破坏操作，窃取了集团内部的敏感信息，现请分析 A 集团提供的系统镜像和内存镜像，找到系统镜像中的恶意软件，分析恶意软件行为。

本任务素材清单：内存镜像 (*.vmem)、存储镜像 (*.img 等)

请按答题卡的要求完成该部分的工作任务。

任务 2：操作系统取证		
序号	任务要求	答案
1	请提交攻击者最后一次执行的命令是什么	
2	请写出桌面上某文件中隐藏的 <i>Flag</i> 信息，提交格式： <i>Flag{...}</i>	
3	请指出内存中恶意进程的 <i>PID</i>	
4	

任务 3：网络数据包分析取证

A 集团的网络安全监控系统发现有恶意攻击者对集团官方网站进行攻击，并抓取了部分可疑流量包。请您根据捕捉到的流量包，搜寻出网络攻击线索，并分析黑客的恶意行为。

本任务素材清单：捕获的网络数据包文件 (*.pcapng、*.pcap 等)

请按答题卡的要求完成该部分的工作任务。

任务 3：网络数据包分析取证		
序号	任务要求	答案
1	请提交攻击者攻击成功的时间，格式： (YYYY-MM-DD HH:mm:ss.SSSSSS)	
2	请指出攻击者上传的恶意文件保存的文件名称（含路径）	
3	请解密服务器返回的加密数据内容	
4	

任务 4：计算机单机取证

对给定取证镜像文件进行分析，搜寻证据关键字（线索关键字为“evidence 1”、“evidence 2”、……、“evidence 10”，有文本形式也有图片形式，不区分大小写），请提取和固定比赛要求的标的证据文件，并按样例的格式要求填写相关信息，证据文件在总文

件数中所占比例不低于 15%。取证的信息可能隐藏在正常的、已删除的或受损的文件中，您可能需要运用编码转换技术、加解密技术、隐写技术、数据恢复技术，还需要熟悉常用的文件格式（如办公文档、压缩文档、图片等）。

本任务素材清单：取证镜像文件（*.e01、*.img 等）

请按答题卡的要求完成该部分的工作任务。

证据编号	在取证镜像中的文件名	镜像中原文件 Hash 码（MD5，不区分大小写）
evidence1		
evidence2		
evidence3		
evidence4		
evidence5		
evidence6		
evidence7		
evidence8		
evidence9		
evidence10		

注：每条证据必须文件名和 Hash 码均答对才得分。

第三部分 应用程序安全

任务 5：应用程序安全分析

A 集团在网络监控过程中发现有可疑的应用程序样本，你的团队需要协助 A 集团对该可疑应用程序进行逆向分析，对黑客攻击的行为进行调查取证，提交相关信息取证分析报告。

本任务素材清单：应用程序文件（ELF、*.exe、*.sys 等）

请按答题卡的要求完成该部分的工作任务。

任务 5：应用程序安全分析		
序号	任务要求	答案

1	请写出恶意程序写入的文件名（不含路径）	
2	请写恶意程序远程通信的服务器域名	
3	请指出恶意程序的破坏行为	
4	

任务 6：代码审计

代码审计是指对源代码进行检查，寻找代码存在的脆弱性，这是一项需要多方面技能的技术。作为一项软件安全检查工作，代码安全审查是非常重要的部分，因为大部分代码从语法和语义上来说是正确的，但存在着可能被利用的安全漏洞，你必须依赖你的知识和经验来完成这项工作。

本任务素材清单：源代码片段（php、c、java）

请按答题卡的要求完成该部分的工作任务。

任务 6：代码审计		
序号	任务要求	答案
1	请指出存在安全问题的代码行（只写一行）	
2	请写出该行代码存在什么漏洞或弱点	
3	

分值分配表

序号	描述	分值
B	网络安全事件响应、数字取证调查、应用程序安全	50
B1	应急响应	11
B2	操作系统取证	9
B3	网络数据包分析取证	9
B4	计算机单机取证	10
B5	应用程序安全分析	9
B6	代码审计	2