四、分析题

26. 计算机安全CIA三元组指的是哪三个方面（3分），并简述对称加密和非对称加密如何实现这三个方面的（7分）？

27. 基于口令的认证中，有256位的哈希值和16位的盐值。用户的口令长度为8个字符，其中每个字符可能是26个小写字母、26个大写字母或10个数字。

（1）给出哈希值的总数量以及盐值的总数量；4

（2）给出口令的总数量；2

（3）攻击者需要进行多少次攻击，请简述具体的攻击过程。4

1. 为了实施 DNS 放大攻击，攻击者必须触发中间服务器产生足够大的 DNS 响应数据包，以超过目标组织网络链路的容量。目标系统的链路带宽是8Mbps。

（1）每个 DNS 响应数据包大小为 1000 字节（忽略封装开销），攻击者每秒必须触发多少个这样的数据包才能淹没该链路？ 3

（2）攻击者发送的请求数据包为60字节，请问占据了链路中多少带宽？3

（3）给出检测DNS放大攻击的两种放大。4

1. 10分
2. 恶意软件的三种传播机制？3
3. 恶意软件的四种有效载荷？2
4. 为了防止恶意软件攻击，如何加固操作系统？5
5. 20分

// php

// 获得用户输入的ID和passwd

$username = 。。。

$password = 。。。

// SQL查询

SELECT username, password FROM users WHERE username = '$username' AND password = '$password';

// 具体代码不记得，大致是这个意思

if ($user && password\_verify($password, $user['password'])) {

// 登录成功（跳转或设置会话）

echo "登录成功！欢迎访问系统。";

// 可添加 session\_start() 和 $\_SESSION 设置

} else {

// 登录失败

echo "登录失败：无效的ID或密码。";

}

注：SQL中，mysql\_real\_escape\_()函数可以转义特殊字符，使其不能发挥作用

1. 上述代码存在什么攻击漏洞，攻击者如何绕过安全检查利用漏洞
2. 除了SQL注入攻击漏洞，还可以利用那些攻击方法并解释原因
3. 如何检测和过滤用户输入（改代码）
4. 给出检测用户输入的一种方法