

单选题

1. Linux命令tracert主要利用了IP协议中的TTL协议字段实现。正确。数据包每经过一次路由ICMP报文头部的TTL字段就减少一个值，这个值等于数据包在路由上消耗的时间（以秒为单位），因为一般这个时间小于一秒，所以基本上每一跳TTL减一。当路由设备收到一个TTL值为0的数据包时，就不再转发，丢弃数据包并向源地址返回一个报错ICMP包。tracert发包时还使用一个非常规的UDP端口，导致即使数据包顺利到达目标主机，目标主机也会返回一个报错的ICMP包。但这个报错包与由于TTL值减为0引起的报错是不同的，tracert依此判断数据包传输情况。tracert通过发送TTL值递增的数据包来记录每一跳的路径，直到TTL值使得数据包恰好达到目标主机。tracert在Windows下命令为tracert。【考察网络相关工具和原理】
2. Linux系统下，进程只能通过系统调用由用户态切换到内核态，并且出于安全考虑，内核态有单独的进程栈空间，不复用用户态栈空间。错误。从用户态到内核态的切换本质上是一个处理中断的过程，表现出来有三种形式：系统调用，外设终端，异常。Linux的每个进程确实有两个栈，分别用于用户态和内核态的进程执行。参考：<https://blog.csdn.net/u014142287/article/details/51934940>；【考察Linux系统基础】
3. 在JavaScript中执行 `encodeURIComponent("hello world!");` 运行结果是 `hello%20world%21`。错误。! 不会被编码。【考察前端基础】
4. 防火墙可以对DDoS攻击提供有效完美的防护过滤。错误。各种防护方案各有优劣，DDoS还没有完美的应对措施。【考察DDoS基础】
5. 在常见Linux场景中，攻击者可以通过篡改CLASSPATH环境变量的方法，向其他程序劫持注入动态链接库。错误。应该是 `LD_PRELOAD`。【考察Linux系统基础】

不定项选择题

应用程序开发过程中，下面哪个是好的安全实践

☐ 使用srand函数初始化后再使用rand函数生成随机数

☐ 使用c标准的系列字符串处理函数strcpy/strcat/sprintf/scanf/gets处理外部输入

☐ 使用system函数执行外部输入的命令

☐ 使用自定义的私有加密算法而不是标准加密算法来增强安全性

AB

- `rand()` 采用线性同余法产生周期极长的伪随机数序列，序列完全取决于其种子。在C标准库中，若没有使用 `srand()` 播种，则默认种子为1，每次生成的是相同的序列，可预测，不安全。
- 安全的加密不应该依赖于算法的保密。

以下程序在64位机器下编译、执行后的输出是

```
#include <iostream>
#include <string>
using namespace std;
int main()
{
    char str[]="This is a string";
    char *ptr=str;
    cout <<ptr<< " ";
    cout <<*str <<" ";
    cout <<sizeof(str) << " " << sizeof(ptr);
    return 0;
}
```

☐ This is a string; This is a string; 16 8

☐ T; This is a string; 17 17

☒ This is a string; T; 17 8

☐ This is a string; T; 16 4

C

- `sizeof()` 操作符用以查询对象或类型的字节数。
-

关于New、 Malloc、 Delete、 Free操作描述不正确的是

☐ 都是在堆上进行动态内存操作的

☐ Malloc在进行内存分配时需要指定字节数，并会对分配的内存进行初始化

☐ New会自动调用对象的构造函数

☐ free 调用是不会自动调用对象析构函数

ABD

- Malloc/Free是标准库函数，New/Delete是C++操作符，成对使用。
- 用Malloc分配内存是在堆上进行，显式指定分配的长度，返回一个void指针，需显式强制类型转换，无初始化。
- New分配内存在自由存储区（free store，抽象概念，可能是堆，静态存储区等）进行，分为new和construct两部分，delete也会进行destruct，free则不会。
- <http://www.cnblogs.com/OG-whz/p/5140930.html>

黑客使用powershell攻击绕过杀毒软件检测，以下说法错误的是

☐ 在系统的applocker中禁用脚本可以防御powershell攻击

☐ 设置powershell的Execution Policy为Restricted，不允许修改的前提下黑客无法执行powershell代码

☐ Applocker可以防护流行的“挖矿”木马

☐ 管理员删除powershell.exe可以防御powershell攻击

AD

- Applocker 不能阻止powershell运行。 <http://drops.xmd5.com/static/drops/tips-11804.html>
- Applocker对木马有一定防护作用，但也存在很多bypass技术。
- powershell是核心组件，不可移除。

IA64 架构下，哪个寄存器是用作栈顶记录

☐ RBP

☐ RIP

☐ RAX

☐ RSP

D

- IA64 架构是原生纯64位，不兼容32位，不像x86-64是基于x86的扩展。IA64的ISA是EPIC (**Explicitly Parallel Instruction Computing，显式并行指令运算**)。
- <http://www.cnblogs.com/bangerlee/archive/2012/05/22/2508772.html>

对于有特定用途的几个寄存器，简要介绍如下：

- * **ax(accumulator)**: 可用于存放函数返回值
- * **bp(base pointer)**: 用于存放执行中的函数对应的栈帧的栈底地址
- * **sp(stack pointer)**: 用于存放执行中的函数对应的栈帧的栈顶地址
- * **ip(instruction pointer)**: 指向当前执行指令的下一条指令

不同架构的CPU，寄存器名称被添以不同前缀以指示寄存器的大小。例如对于x86架构，字母“e”用作名称前缀，指示各寄存器大小为32位；对于x86_64寄存器，字母“r”用作名称前缀，指示各寄存器大小为64位。

tcp协议状态变迁, 在ESTABLISHED状态下主动发送FIN时, 进入哪个状态

☐ TIME_WAIT

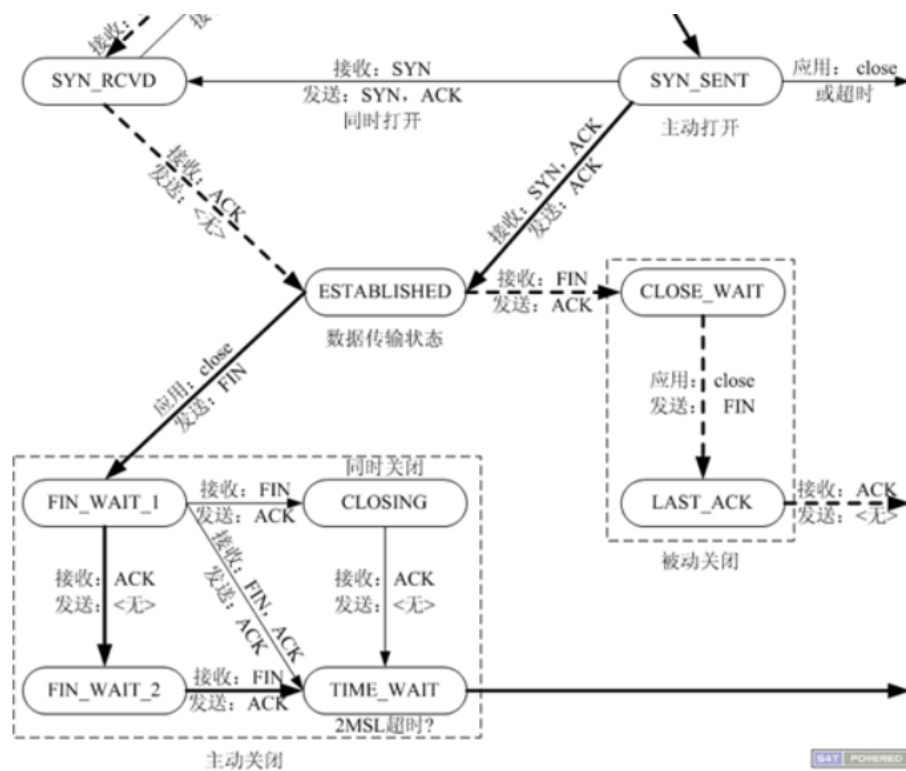
☐ FIN_WAIT

☐ CLOSING

☐ CLOSE_WAIT

B

- <http://blog.smallmuou.xyz/network/2017/03/24/TCP%E7%8A%B6%E6%80%81%E5%9B%BE.html>
- <https://coolshell.cn/articles/11564.html>
- TCP协议状态机 http://www.tcpiptide.com/free/t_TCPOperationalOverviewandtheTCPFiniteStateMachineF-2.htm



近段时间Memcache出现漏洞被利用发起大规模攻击，主要是利用哪个协议进行攻击

☐ ICMP

☐ TCP

☐ UDP

☐ SNMP

C

对于C++程序而言，编译成EXE后可以发现，通常局部变量的初始值会存放在___，而全局变量的初始值会存放在___

☐ 堆，栈

☐ 栈，text区

☐ 堆，code区

☐ 栈，堆

B

<https://blog.csdn.net/yangquanhui1991/article/details/51786380>

在Debian中，想要查看PID为1000的进程的内存布局，请补全命令缺失的部分：cat _____/maps

☐ /etc/1000

☐ /proc/pid/1000

☐ /proc/1000

☐ /etc/pid/1000

C

对于ARM指令MOV R1,R0,LSL #2，已知R0的值为7，R1的值为5，R2的值为3。那么这步操作执行完以后R1的值为？

☐ 15

☐ 35

☐ 21

☐ 28

D LSL 是左移，等价于 $R1=R0 \ll 2$ 。

64位程序的char*（字符串类型指针）、函数指针、int32_t*类型分别占用多少个字节的内存

☐ char*类型占用最小

☐ 三种类型不同，所以占用内存也不同

☐ 函数指针和int32_t*占用内存相同

☐ char*占用8字节

?

全局变量BYTE X = 4，线程A、B、C几乎同时执行的依次执行(1) MOV EAX, X (2) INC EAX (3) MOV X, EAX这三条指令，导致了“条件竞争”的安全问题，请写出三个线程执行完之后，所有可能的值

☐ 4, 4, 5

☐ 5, 5, 5

☐ 4, 5, 6

☐ 5, 5, 6

?

下面哪个不属于防御json劫持的办法？

☐ Cookie鉴权

☐ Referer校验

☐ CSRF Token

☐ 以上都不属于

ABC

json劫持是CSRF的一种。

<http://drops.xmd5.com/static/drops/papers-42.html>

<http://www.cnblogs.com/xusion/articles/3107788.html>

http://blog.knownsec.com/2015/03/jsonp_security_technic/

<https://shiyousan.com/post/635445288414621221>

常用于网页挂马的 HTML 标签不包括下面哪一个？

☐ <iframe>

☐ <script>

☐ <body>

☐ <select>

D

访问http://aq.qq.com/cn2的过程中，HTTP 响应包 HEADER 中某个字段为 Set-Cookie: test3=123; HttpOnly，那么下面哪个是`test3` 的生效范围？

☐ domain: .aq.qq.com, path: /

☐ domain: .qq.com, path: /

☐ domain: .aq.qq.com, path: /cn2

☐ domain: .qq.com, path: /cn2

C

默认path是设置cookie的页面的path，默认domain是设置cookie页面的domain及其子域。

避免程序出现上传文件漏洞，下列哪个是正确的处理办法？

☐ 前端限制上传文件后缀

☐ 后端限制上传文件后缀

☐ 前端限制上传文件MIME类型

☐ 后端限制上传文件MIME类型

D

PHP中，下列哪个函数不可以用来防御针对字符串型参数的SQL注入攻击？

☐ stripslashes

☐ mysql_escape_string

☐ mysql_real_escape_string

☐ addslashes

A

请问下列哪个 URL 与http://aq.qq.com/cn2/index满足浏览器的“同源策略”？

☐ https://aq.qq.com/cn2/index

☐ http://aq.qq.com:80/cn2/ipwd/my_ipwd

☐ http://www.aq.qq.com/cn2/index

☐ https://aq.qq.com/cn2/ipwd/my_ipwd

B

https与http协议不同；C的主机名是www，与题干URL的host不同。

以下说法正确的是？

☐ 可以通过ping 服务器的53端口来判断服务器是否开启DNS服务

☐ HTTP服务器遭受UDPFLOOD，通常表现CPU 100%

☐ rst报文不能用于DDoS攻击

☐ 反射攻击主要用于阻塞带宽

BD

<http://www.jdfhq.com/Display.aspx?ID=42>

以下说法正确的是？

☐ cc攻击会造成数据泄露

☐ 公司办公出口IP遭受DNS反射攻击时，可以直接通过封禁UDP源端口53的流量解决

☐ SNMP反射攻击是TCPFLOOD的一种

☐ 伪造源IP无法发起有连接的HTTP GET FLOOD

B

<https://blog.csdn.net/lanyd/article/details/54976294>

关于反射放大攻击，下列正确的是

☐ 任意协议都可被用作反射放大攻击

☐ 返回的数据量要大于请求的数据量

☐ 通常可放大几十倍到上百倍

☐ 封堵ip的方式可以有效防御反射放大攻击

BC

TCP协议的数据单元被称为

☐ 比特

☐ 帧

☐ 分段

☐ 字符

ABC D

bit,frame,packet,segment,data

一般哪些服务常被用来做反射攻击

☐ DNS服务

☐ NTP服务

☐ Memcached服务

☐ HTTP服务

ABC

网络服务器网卡接口充满大量请求信息，带宽满载，导致系统无法正常服务，这最可能遭受什么攻击？

☐ SQL注入

☐ DDoS攻击

☐ APT攻击

☐ 反射放大攻击

BD

黑客登录SSH，哪个日志文件会记录？

☐ access.log

☐ secure

☐ boot.log

☐ wtmp

BD

https://blog.csdn.net/oxford_d/article/details/51820031

下面哪款工具不能用于反弹shell？

☐ Netcat

☐ Dnscat

☐ meterpreter

☐ maltego

ABC

<https://xz.aliyun.com/t/2214>

下面哪起事件中恶意代码使用了DNS隧道通信？

☐ Xcode Ghost后门事件

☐ XShell后门事件

☐ CCleaner后门事件

☐ Elmedia Player后门事件

B

redis无鉴权可能造成getshell，其默认开放端口是？

☐ 1433

☐ 53

☐ 6379

☐ 11211

C

以下哪款工具不具备远程控制功能？

☐ 灰鸽子

☐ hydra

☐ pupy

☐ cobaltstrike

ACD

以下哪款工具为系统密码提取工具？

☐ nmap

☐ hashcat

☐ burpsuite

☐ mimikatz

D

填空题

1. PHP用来过滤命令注入的两个函数是？和？。

→ ↺ ↻

php.net/manual/en/ref.exec.php

php

Downloads

Documentation

Get Involved

Help

safe_mode_exec_dir directive.

Table of Contents

escapeshellarg

— Escape a string to be used as a shell argument

escapeshellcmd

— Escape shell metacharacters

exec

— Execute an external program

passthru

— Execute an external program and display raw output

proc_close

— Close a process opened by proc_open and return the exit code of that process

proc_get_status

— Get information about a process opened by proc_open

proc_nice

— Change the priority of the current process

proc_open

— Execute a command and open file pointers for input/output

proc_terminate

— Kills a process opened by proc_open

shell_exec

— Execute command via shell and return the complete output as a string

system

— Execute an external program and display the output

- 按照漏洞触发方式的不同，XSS漏洞可分为三类，分别是？、？和？。【反射型XSS、存储型XSS和DOM-base型XSS】
- 填写一下反射攻击报文的源端口：SSDP反射，源端口为1900；Memcache反射，源端口为？【11211】
- 在进行网络分析时，可使用？命名来测试主机到目标主机之间所经过的所有路由器路径。【traceroute】
- 在常规的Linux场景中，程序员或攻击者可以通过篡改？环境变量的方法，劫持其他程序调用libc函数库。【LD_PRELOAD】
- 在Linux文件的时间格式中，如果一个文件的属主信息发生变更，则会更新该文件的？时间标志字段。【mtime】 http://blog.sina.com.cn/s/blog_6e6d706501010r2f.html
- 在Windows的内网入侵渗透过程中，攻击者可以使用Windows自带的？序进行端口转发。【netsh】


附加题

 [附加题|10分]

题目描述

你需要黑入一个广泛被采用的智能门禁系统。这个门禁系统搭载Debian操作系统，与它的服务器通过Wifi连接，也通过无线网络与区域内其他智能设备相连。它进行人脸识别及虹膜识别以自动放行。你如何才能使得该系统对不在允许名单中的你进行放行，思路是什么？（社工除外）

 如需画图或推导，你可以在草稿纸上作答，手机拍照后[点此扫码上传](#)

代码语言 

- 当门禁处于放行状态时，通过物理手段屏蔽该区域Wifi信号，暂时中断系统和服务器的通信。
- 尝试接入门禁系统所用Wifi，嗅探流量以熟悉数据报文格式。伪造相同id的热点迫使设备重连到虚假Wifi，伪造响应报文。
- 尝试接入门禁系统所用Wifi，尝试通过arp欺骗实现中间人攻击。
- 尝试接入门禁系统所用Wifi，探测操作系统开放端口和服务，探测区域内其他智能设备开放的端口和服务，进一步攻击。

🔍 [附加题|10分]

题目描述

PHP和MySQL环境下，当接收的参数值中单引号、双引号以及小括号都被过滤的情况下，是否可以防御SQL注入拖库？有哪些防御SQL注入拖库的解决方案？请列举三种或以上方案，并简述其实现原理。

📌 如需画图或推导，你可以在草稿纸上作答，手机拍照后[点此扫码上传](#)

代码语言 ▼ **B** **I** U “ ” ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ x_2 x^2 Σ π

不能彻底防御。如果注入点是数字型注入则不需要引号闭合，因此不能；如果注入点是字符型，也可能存在多点注入，从而根据拼接处上下文，利用注释打通多点注入。

防御方案：

- 1.使用预编译查询语句。通过对将要用到的查询语句进行预编译，使用时以格式化填充参数，达到分离数据和代码的目的。
- 2.过滤用户输入。通过使用有效的waf，过滤敏感字词（单双引号，注释符，分号、空字符等分隔符，select等sql语句关键字），净化用户输入，使得最终执行的查询时无害的。
- 3.安全配置数据库。遵循最小权限原则，使用低权限用户执行数据库操作，禁止查询包含数据库元数据的表，如information_schema等。

🔍 [附加题|10分]

题目描述

就最近比较热门的软件供应链安全和区块链安全，应该如何应对？可选一个熟悉的话题，谈谈你的看法。

📌 如需画图或推导，你可以在草稿纸上作答，手机拍照后[点此扫码上传](#)

代码语言 ▼ **B** **I** U “ ” ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ x_2 x^2 Σ π

字数：0

⚠ 重要提醒:

- 1 本目录页为本场考试的全部题型，你可从任一部分开始作答，进入后需作答完毕，提交该部分答案才可返回目录页，答案提交后无法返回修改。
- 2 答题过程中全程摄像头开启，并会记录你的做题路径。

单选题	5题	满分10分		已提交
不定项选择题	30题	满分75分	少选不得分	已提交
填空题	7题	满分15分		已提交
附加题	3题	满分30分		已提交