360 网络安全职业技能大赛初赛理论分赛

1.（单选题）
如果使用 sqlmap 进行注入时需要指定注入技术，则需要使用哪个参数（）（4 分）
A —dbs
B —risk
C —Level
D —technique
2.（单选题）
网站文件存放在/www/html/ 目录下，且页面中包含 include($_GET[‘page’]); 关键代码，以下哪个选项不可以获得 linux 系统中自有的 passwd 文件内容（）（4 分）
A ?page=../etc/passwd
B ?page=../../../etc/passwd
C ?page=../../../../../etc/passwd
D ?page=../../../../../../etc/passwd
3.（多选题）
IIS6.0 存在的文件解析漏洞，是由于哪些特殊符号导致利用（）（4 分）
A :
B ;
C @
D /
4.（单选题）
RSA 算法，在以下哪种特定场景相对安全（）（4 分）
A e 很大
B p 和 q 很大，但相近
C e 很小
D n 很大
5.（单选题）
下列哪项为 nmap 使用 ICMP 进行 C 段扫描，但不进行扫描端口和 DNS 反向查询（）（4 分）
A nmap -Pn -sn -n 192.168.1.1/24
B nmap -Ss -sn -n 192.168.1.1/24
C nmap -sn 192.168.1.1/24
D nmap -PE -sn -n 192.168.1.1/24
6.（多选题）
以下方法中可能存在命令执行漏洞的有（）（4 分）
A string shell_exec (string $cmd)
B string exec (string $command [, array &$output [, int &$return_var]])
C void passthru (string $command [, int &$return_var])
D string escapeshellarg (string $arg)

7.（单选题）
PHP 错误页面信息不包括（）（4 分）
A 语法错误信息
B 出错文件所在位置
C 错误信息所在行
D PHP 版本信息
8.（多选题）
只允许 192.168.1.80/32 访问某 Linux 主机，可采用（　　）方法实现。（4 分）
A 本机防火墙
B 网络防火墙
C 本机 hosts.allow 文件
D 本机 hosts.deny 文件
9.（单选题）
这段代码是以下哪种漏洞类型的 payload（）
Runtime.getRuntime().exec(request.getParameter("cmd")); （）（4 分）
A SQL 注入漏洞
B 命令执行漏洞
C XSS 跨站漏洞
D 文件读取漏洞
10.（单选题）
DDOS 反射攻击中，下面哪项协议拥有最大的反射倍数（）（4 分）
A DNS
B MEMCACHE
C TFTP
D SNMP
11.（单选题）
Apache 解析文件的机制是（）（4 分）
A 不允许多个点分割的后缀，从右向左解析
B 允许多个点分割的后缀，从右向左解析
C 不允许多个点分割的后缀，从右向左解析并裁剪不存在的路径
D 允许多个点分割的后缀，从右向左解析并裁剪不存在的路径
12.（单选题）
metasploit 使用 ms17-010 攻击机器哪个端口服务（）（4 分）
A 445
B 139
C 135
D 1025
13.（单选题）
导致 Tomcat 任意文件上传漏洞(CVE-2017-12615)的原因是（）（4 分）
A 允许 POST 请求方法
B 允许 OPTIONS 请求方法
C 配置文件中 readonly 参数设置为 false
D 配置文件中 readonly 参数设置为 true

14.（单选题）
文件包含漏洞可以与以下哪个漏洞配合，实现 Getshell（）（4 分）
A 逻辑漏洞
B 上传漏洞
C 信息泄露
D 反射型 XSS
15.（单选题）
当用户在浏览器中输入一个需要登录的网址时，系统先去哪里查询 IP 地址？（4 分）
A 本地域名服务器
B 顶级域名服务器
C 根域名服务器
D hosts 文件
16.（单选题）
下面哪种处理文件上传的方式不够妥当 （）（4 分）
A 通过黑名单验证上传的文件后缀名称
B 设置上传目录不可解析
C 重命名上传的文件名称
D 使用单独的服务器存放上传的文件
17.（单选题）
目标计算机与网关通信失败，同时导致通信重定向的攻击形式是以下哪种攻击？（4 分）
A 病毒
B 木马
C DOS
D ARP 欺骗
18.（单选题）
关于文件解析描述正确的是（）（4 分）
A 文件解析过程就是读取文件内容的过程
B 文件解析就是找到文件存放路径的过程
C 文件解析是找到能处理该文件应用的过程
D 文件解析由操作系统负责
19.（单选题）
DNS 系统 NS 记录主要作用（）（4 分）
A 主机 IP 地址
B 域名服务器记录
C 域名说明
D 邮件交换记录
20.（单选题）
我们在浏览器看到的 web 服务器证书中，包含了（）（4 分）
A 服务器的公钥
B 服务器的私钥
C 客户端浏览器的公钥
D 客户端浏览器的私钥

21.（单选题）
在 IPSec 中，（ ）协议既可以实现数据加密，又可以实现数据完整性验证和数据源身份认证。（4 分）
A AH
B GRE
C MPLS
D ESP
22.（多选题）
对于 SQL 注入攻击的防御，可以采取哪些措施（）。（4 分）
A 不要使用管理员权限的数据库连接，为每个应用使用单独的权限有限的数据库连接。
B 不要把机密信息直接存放数据库，加密密码和敏感的信息。
C 不要使用动态拼装 sql，可以使用参数化的 sql 或者直接使用存储过程进行数据查询存取。
D 对表单里的数据进行验证与过滤，在实际开发过程中可以单独列一个验证函数，该函数把每个要过滤的关键词如 select，1=1 等都列出来，然后每个表单提交时都调用这个函数。
23.（单选题）
GIT 版本控制系统添加文件到仓库以后，文件会被存储到仓库哪个文件夹（）（4 分）
A source
B warehouse
C objects
D pristine
24.（单选题）
内网横向移动时经常利用的 GPP 漏洞,和 Windows 系统的哪一项组件密切相关()。（4 分）
A 注册表
B SMB 服务
C 组策略
D 本地安全策略
25.（单选题）
采用 TCP/IP 数据封装时，以下哪个端口号范围标识了所有常用应用程序（4 分）
A 0 到 255
B 256 到 1023
C 0 到 1023
D 1024 到 2047
26.（单选题）
在 DDOS 攻击中，TCP 的 SYN 攻击主要利用了 TCP（）原理 （4 分）
A 滑动窗口
B 三次握手
C 四次挥手
D 流量控制

27.（单选题）
通过 TCP 序号猜测，攻击者可以实施下列哪一种攻击（4 分）
A 端口扫描攻击
B ARP 欺骗攻击
C 网络监听攻击
D TCP 会话劫持攻击
28.（单选题）
关于以下函数描述正确的是（）（4 分）
A eval()函数将输入的内容作为系统命令执行
B assert()函数作用与 eval()函数相同
C exec()函数返回执行结果的全部数据
D shell_exec()函数返回执行结果的最后一行数据
29.（单选题）
以下哪个是具备 htmlEncode 功能的标签（）（4 分）
A
B <script></script>
C <iframe></iframe>
D <a>
30.（单选题）
在 windows 域中，如果想使用 kerberos 身份验证，一般流程是（）（4 分）
A 客户端申请获得票据许可票据（TGT），客户端申请获得服务许可票据（SGT），客户申请获得服务许可访问服务器。
B 客户端申请获得服务许可票据（SGT），客户端申请获得票据许可票据（TGT），客户申请获得服务许可访问服务器。
C 客户端申请获得服务许可访问服务器，客户端获得票据许可票据（TGT），客户端申请获得服务许可票据（SGT），客户访问服务器。
D 服务端申请获得服务许可访问服务器，服务端获得票据许可票据（SGT），服务端申请获得服务许可票据（TGT），服务端推送服务至客户端。
31.（多选题）
php://filter/read=convert.base64-encode/resource=../../../../../etc/passwd
假设某 PHP 页面存在文件包含漏洞，上述 Payload 可以获得哪些信息（）（4 分）
A Linux 系统中所有的用户名
B Windows 系统中所有的用户名
C 系统中各个用户的权限以及可执行文件所在目录
D 用户密码
32.（单选题）
下列选项不属于信息安全三要素的是哪一项？（4 分）
A 机密性
B 可抵赖性
C 完整性
D 可用性

33.（多选题）
Windows 7 系统中，创建隐藏账户 hider 的主要步骤包括（）。(4 分)
A 创建用户 hider
B hider 键值导入注册表
C 删除 hider
D 导出 hider 键值
34.（单选题）
ARP 欺骗的实质是哪一选项？（4 分）
A 提供虚拟的 MAC 与 IP 地址的组合
B 让其他计算机知道自己的存在
C 窃取用户在网络中的传输的数据
D 扰乱网络的正常运行
35.（单选题）
当请求资源不存在是，返回的响应码是？（4 分）
A 400
B 401
C 403
D 404
36.（多选题）
在 Mysql 数据库中，基于时间的盲注常使用的延迟函数有（）(4 分)
A benchmark（）函数
B substr（）函数
C sleep（）函数
D hash（）函数
37.（多选题）
通用入侵检测模型（CIDF）中包含下列哪些组件？（ ）(4 分)
A 事件产生器
B 事件分析器
C 响应单元
D 事件数据库
38.（单选题）
密码学在区块链的应用中，工作量证明主要使用下面哪种算法（）(4 分)
A 对称加密算法
B 哈希算法
C 非对称加密算法
D 密钥交换算法
39.（多选题）
操作系统安全机制包括（）。(4 分)
A 访问控制
B 安全审计
C 运行保护
D 硬件保护

40.（单选题）
阻止恶意文件上传比较有效的方法是（）（4 分）
A 白名单后缀
B 黑名单后缀
C 过滤敏感字符
D 替换敏感字符
41.（单选题）
802.11 采用的 WEP 加密所使用的核心加密算法（）（4 分）
A AES
B RC4
C MD5
D DES
42.（单选题）
IP 地址中 B 类地址具有多少位主机号？（4 分）
A 8
B 16
C 24
D 31
43.（单选题）
下列措施中不能增强 DNS 安全的是哪一选项？（4 分）
A 使用最新的 BIND 工具
B 双反向查找
C 更改 DNS 的端口号
D 不要让 HINFO 记录被外界看到
44.（单选题）
以下哪种方法在 PHP 开发语言中不能执行命令（）（4 分）
A system(whoami);
B system('whoami');
C system('eval(whoami);');
D eval('system(whoami);');
45.（单选题）
在 windows 域中，如果想使用 kerberos 身份验证，服务实例需要注册一个什么（）（4 分）
A SPN
B PTK
C Session
D Cookie
46.（单选题）
IP 协议工作在 TCP/IP 的哪一层？（4 分）
A 物理层
B 链路层
C 网络层
D 传输层

47.（多选题）
域树在两个域之间的关系可以是（）。(4 分)
A 不可传递信任关系
B 双向信任关系
C 单向信任关系
D 可传递信息关系
48.（单选题）
BASE64 编码的 64 个字符中，不包含( )　(4 分)
A +
B /
C =
D 0
49.（单选题）
产生 CSRF 漏洞的原因是（）(4 分)
A 对用户的输入没有做过滤
B 对 IP 地址没有做限制
C 对用户的敏感操作缺乏二次验证
D 对用户的 cookie 缺乏验证
50.（单选题）
网络监听（嗅探）的这种攻击形式破坏了下列哪一项内容（4 分）
A 网络信息的抗抵赖性
B 网络信息的保密性
C 网络服务的可用性
D 网络信息的完整性
51.（多选题）
哪些场景容易出现 SSRF 漏洞（）(4 分)
A 分享
B 上传
C 收藏
D 翻译网页
52.（多选题）
使用 00 截断绕过文件上传检测，需要注意的是（）(4 分)
A php 版本小于 5.3.4
B magic_quotes_gpc 参数为 off
C 业务系统是否适合使用 00 截断
D 上传文件添加十六进制图片头
53.（单选题）
关于命令执行漏洞的描述，正确的是（）(4 分)
A 命令执行漏洞仅存在于 C/S 架构中
B 命令执行漏洞危害不大
C 命令执行漏洞与用户输入无关
D 大多数脚本语言都可以调用操作系统命令

54.（多选题）
下列哪些方式可以收集子域名（）（4 分）
A 爆破
B 利用搜索引擎挖掘
C 利用域传送漏洞
D 利用 CSRF 漏洞
55.（多选题）
跟 Windows 的账号密码存储有关的文件有（）（4 分）
A LM-Hash
B /etc/password
C NTLM-Hash
D SAM
56.（单选题）
下面哪个字段是 HTTP 请求中必须的？（4 分）
A Cookie
B Host
C Accept
D Content-Length
57.（单选题）
内网渗透中经常使用到 Metasploit 平台的 Meterpreter 模块属于()功能的组件。（4 分）
A 编码模块
B 攻击载荷模块
C 空指令模块
D 后渗透攻击模块
58.（单选题）
使用 DDOS 攻击 WEB 中某一链接时，最好的防御思路是（4 分）
A 加入验证码，识别机器发送流量
B 使用流量清洗设备
C 购买抗 DDOS 防火墙
D 移除 WEB 中的链接
59.（多选题）
下列哪些是 DNS 的记录类型（4 分）
A A
B AAAA
C NS
D HINFO

60.（单选题）
RSA 算法，已知 p=7，q=17， e=5 则 d 可能为（）（4 分）
A 67
B 61
C 77
D 73

61.（多选题）
实现 XSS 蠕虫常用的技术有（）（4 分）
A DOM
B Ajax
C 社会工程学
D SQL 语法
62.（单选题）
GIT 版本控制系统，添加到仓库文件所使用哪种编码进行压缩文件（）（4 分）
A ASCII
B Zlib
C Gz
D Bz
63.（单选题）
关于入侵检测系统，下列说法正确的是（ ）。（4 分）
A 入侵检测系统可以检测到所有的入侵行为
B 入侵检测系统不可避免存在误报问题
C 入侵检测系统可以对网络数据包进行过滤
D 入侵检测系统只支持 TCP、UDP 及其之上的应用层协议
64.（多选题）
网络入侵检测系统（NIDS）可根据（ ）等特征检测和识别网络入侵行为。（4 分）
A IP 地址与端口号
B TCP 标志位
C 数据包长度
D 数据包中的特定字符串
65.（单选题）
HTTP 协议返回 Server 字段中可以提取下列哪项信息（）（4 分）
A 数据库信息
B 操作系统内核
C 用户请求的 User-Agent
D 中间件服务
66.（单选题）
当今，流行的 DDOS 攻击主要以攻击（）为主要目标 （4 分）
A 存储资源
B CPU 资源
C 内存资源
D 网络资源
67.（单选题）
Windows10 操作系统上比较重要的一项安全策略 UAC 策略的主要作用是（）。
（4 分）
A 密码访问控制
B 密码访问策略
C 用户账户控制
D 账户访问控制

68.（单选题）
将 MAC 地址转换为 IP 地址的协议是？ （4 分）
A ARP
B RARP
C IP
D NTP
69.（单选题）
关于文件解析防御的说法，不正确的是（）（4 分）
A 文件解析漏洞是因为配置错误导致，采用安全的配置就能防御文件上传
B 系统开发过程中开启的便利功能，在上线前要严格检查
C 在防御文件上传漏洞的同时也要留意其他漏洞
D 及时更新中间件版本，补丁
70.（单选题）
在防火墙中,可利用( )技术实现 IP 地址复用以及隐藏内部网络 IP 地址的功能。（4 分）
A 包过滤
B 代理服务
C NAT
D 状态检测
71.（单选题）
OSI 参考模型分几层？（4 分）
A 4
B 5
C 6
D 7
72.（多选题）
LAMP 下的 WEB 网站加固方法包括（ ）。（4 分）
A 升级 Linux 版本并进行安全加固
B 禁止上传文件
C 上传目录去掉执行权
D 仅允许上传图片文件
E 以一般用户运行 apache 服务器
73.（单选题）
SQL 注入主要危害的是什么组件里面的信息（）。（4 分）
A 内存堆栈
B 数据库
C HTML 页面
D 浏览器
74.（单选题）
Active Directory(活动目录)中的数据库文件是（）？（4 分）
A NTDS.dit
B SAM.dit
C PASS.dit
D USER.dit

75.（单选题）
https 是指以下哪种协议？（4 分）
A TLS/SSL 加密的 HTTP 协议
B TLS/SSL 加密的 DNS 协议
C TLS/SSL 加密的 SMTP 协议
D TLS/SSL 加密的 POP3 协议
76.（多选题）
上传文件后缀检测，常见的方法有（）（4 分）
A JS 调用 select()函数
B PHP 调用 pathinfo()函数
C getimagesize() 函数
D PHP addslashes()函数
77.（单选题）
（ ）是一种在互联网上运行的计算机系统，它是专门为吸引并诱骗那些试图非法闯入他人计算机系统的人（如黑客）而设计的。（4 分）
A 傀儡计算机
B 入侵检测系统
C 蜜罐
D 入侵防御系统
78.（单选题）
DDOS 的大流量攻击中，主要是（）报文比较多（4 分）
A TCP
B UDP
C ICMP
D 广播
79.（单选题）
Windows 域中，使用 kerberos 身份验证过程中的 PTT 传递的是（）（4 分）
A 哈希
B 票据
C 密码
D 服务
80.（单选题）
宽字节注入利用漏洞原理主要是基于（）（4 分）
A 汉字编码中 gbk 和 uft-8 的不统一
B 数据库对输入长度控制不严引起
C URL 提交请求中的特殊符号引起
D URL 提交请求中的大小写没有过滤引起
81.（单选题）
以下哪个文件格式是利用 nginx 解析漏洞的（）（4 分）
A /test.asp;1.jpg
B /test.jpg/test.php
C /test.asp/test.jpg
D /test.php.xxx

82.（单选题）
TCP 协议建立连接需要几次握手？（4 分）
A 2
B 3
C 4
D 5
83.（单选题）
已知上级目录下的 db 目录包含敏感文件 db.rar，以下哪个请求可以下载到该文件（）（4 分）
A ?download=db.rar
B ?download=../db/db.rar
C ?download=db/db.rar
D ?download=./db/db.rar
84.（多选题）
HTTP 返回下列哪些状态码证明目录存在（）（4 分）
A 200
B 403
C 404
D 401
85.（单选题）
“防火墙的物理接口均未配置 IP 地址，它在网络中的作用相当于一台二层交换机”。根据以上描述判断，该防火墙最有可能工作在（ ）模式。（4 分）
A 路由
B 透明（桥接）
C 冗余
D 混合
86.（单选题）
nmap -PS 扫描参数具体含义（）（4 分）
A 使用 SCTP 扫描主机存活
B 使用 TCP Syn 扫描主机存活
C 使用 TCP Syn 扫描端口开放
D 使用 Ping 探测主机存活
87.（多选题）
IPSec VPN 的数据封装模式包括（ ）。（4 分）
A 传输模式
B 路由模式
C 加密模式
D 隧道模式
88.（单选题）
利用虚假 IP 地址进行 ICMP 报文传输的攻击方法称为什么攻击？（4 分）
A ICMP 泛洪
B 死亡之 ping
C LAND 攻击
D Smurf 攻击

89.（单选题）
内网 linux 系统中常使用 scp 命令在网络上的主机之间复制文件。 它使用（）协议进行数据传输（4 分）
A FTP
B Telnet
C IPC
D SSH
90.（单选题）
防御 XSS 漏洞的核心思想为（）（4 分）
A 禁止用户输入
B 输入过滤，输出编码
C 要点击未知链接
D 减少使用数据库

91.（多选题）
SQL 查询语句 Select * from users Where id=1 为了防止被 SQL 注入利用，通过正则算法把“=”号给过滤不让使用了，那么可以使用 sqlmap 的 tamper 目录下的哪些脚本调用来绕过正则检测进行 SQL 注入？（）（4 分）
A randomcase.py
B equaltolike.py
C charencode.py
D space2comment.py

92.（单选题）
一般来说，包过滤防火墙依据网络数据包的（ ）执行包过滤规则。（4 分）
A 包头信息
B 有效载荷信息
C 源 IP 地址
D 状态信息

93.（单选题）
以下哪项是开源网络入侵检测工具？（ ）（4 分）
A Nessus
B Nmap
C Iptables
D Snort

94.（多选题）
Linux 系统账户密码策略加固方法包括（ ）。（4 分）
A 账户名长度限制
B 密码字符类型限制
C 密码最小长度限制
D 密码使用时间限制
E 限制使用历史密码

95.（单选题）
下面哪种方式可以进行 TCP 的流量控制?（4 分）
A 滑动窗口
B 超时重传
C 停止等待
D 重传机制
96.（单选题）
nmap 使用半开放扫描时，若目标端口开放则第三次握手主机将向目标机发送什么标志（）（4 分）
A SYN
B ACK
C RST
D FIN
97.（单选题）
UDP 工作在 TCP/IP 的哪一层?（4 分）
A 传输层
B 网络层
C 物理层
D 应用层
98.（单选题）
文件包含漏洞的一般特征不包含（）（4 分）
A ?page=a.php
B ?home=a.html
C ?file=content
D ?id=1’
99.（单选题）
Vim 第一次异常退出后，会产生下列哪个异常文件（）（4 分）
A .swp
B .swo
C swq
D swn
100.（单选题）
SVN 客户端仓库文件中，哪个文件用来记录添加仓库源文件名（）（4 分）
A log.txt
B index
C head.db
D wc.db