多选测试模拟试卷

考试时间：2024-03-20 16:00-22:00  
总分：120

|  |  |
| --- | --- |
| 总分 |  |

一、单选题

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 题号 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 答案 |  |  |  |  |  |  |  |  |  |  |

1. 你在逛商场时发现手机没有流量，正好看到WiFi列表里有一个某咖啡店的公共WiFi，你会（4分）

A、连接  
B、不连接

2. DDos的常见攻击手段不包括（）？（4分）

A、流量带宽消耗  
B、挖断该企业的网络光纤  
C、主机资源消耗  
D、利用拒绝服务漏洞攻击

3. 应用如果要收集用户的数据，（）？（4分）

A、可预留后门远程操控用户终端  
B、征得用户同意即可收集全部隐私信息  
C、征集用户同意收集功能相关数据  
D、无须征得同意即可收集数据

4. 下列哪一种类型的防火墙的使用到的技术最简单，且出现的最早？（4分）

A、应用防火墙  
B、代理防火墙  
C、状态检测防火墙  
D、包过滤防火墙

5. 网络安全法中触发的金额最高可达（）万元？（4分）

A、10  
B、50  
C、100  
D、80

6. 下面哪个选项不是IPS的特性？（4分）

A、能够实时监控多种网络攻击并进行阻断  
B、使用DPI技术，深入七层的数据流攻击特征，依靠静态签名识别攻击  
C、旁路接入网络即可保护网络  
D、在线部署，实施阻断攻击

7. 魏则西案后（）这个最关键的影响因素依然存在？（4分）

A、广告等标识符不清楚  
B、搜索引擎竞价排名  
C、无良医疗广告夸大其辞  
D、诈骗电话

8. DDos的常见攻击手段不包括（）？（4分）

A、流量带宽消耗  
B、挖断该企业的网络光纤  
C、主机资源消耗  
D、利用拒绝服务漏洞攻击

9. WEB防篡改系统如何实现的（）？（4分）

A、降低中间件权限使其失去对网页文件的更改权限  
B、通过CDN代理的方式避免网站被getshell进行篡改  
C、有监控程序检测并禁止非授权的首页更改  
D、使站点直接成为纯静态网页

10. 下面哪个选项不是IPS的特性？（4分）

A、能够实时监控多种网络攻击并进行阻断  
B、使用DPI技术，深入七层的数据流攻击特征，依靠静态签名识别攻击  
C、旁路接入网络即可保护网络  
D、在线部署，实施阻断攻击

|  |  |
| --- | --- |
| 总分 |  |

二、多选题（少选得一半分）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 题号 | 1 | 2 | 3 | 4 | 5 |
| 答案 |  |  |  |  |  |

11. 运维安全审计的主要功能应该包含（）？（4分）

A、单点登录  
B、身份认证  
C、操作审计  
D、违规操作阻断

12. 从系统层次上讲，网络安全实质上包含哪三个层次（）？（4分）

A、物理安全  
B、人员安全  
C、网络安全  
D、信息安全

13. SYN洪水攻击中涉及含什么标志位的包？（4分）

A、SYN  
B、SYN-ACK  
C、ACK  
D、FIN

14. 以下哪些协议与电子邮件协议有关？（ ）（4分）

A、HTTP  
B、IMAP  
C、POP  
D、SMTP

15. 下面关于 ARP 协议的描述中，错误的是（ ）。（4分）

A、ARP协议根据IP地址获取对应的MAC地址  
B、ARP报文封装在IP数据报中传送  
C、ARP请求采用单播方式，应答使用广播方式  
D、ARP协议是一种路由协议

|  |  |
| --- | --- |
| 总分 |  |

三、简答题

16. 简述震网病毒感染到主机的行为特征？以及震网病毒的特点及启示？（10分）

17. 简述2010年震网病毒如何投递到伊朗核电站，并如何进行攻击致使离心机报废？（10分）

|  |  |
| --- | --- |
| 总分 |  |

四、论述题

18. 遇到文件包含场景漏洞题目，如何进行远程文件包含攻击？阐述攻击过程及原因。（20分）

19. 描述基于联合查询注入的SQL注入过程，给出每步详细的payload和思路简述。（20分）