# 单选（15\*1）

# 二、填空（20\*1）

1、Kali的主要功能有（）（）和（）。

数字取证、安全审计、渗透测试

2、安全审计涉及的四个基本要素是（）（）（）和（）。

控制目标、安全漏洞、控制措施、控制测试

3、渗透测试可分为（）（）和（）三种。

黑盒测试、白盒测试、灰盒测试

4、数字取证处理的对象是（），是指以存储的电子化信息资料来证明案件真实情况的电子物品或电子记录。

电子证据

5、Kali系统默认的登陆账号是（），密码是（）。

root、toor

6、VMware虚拟机连接有线网络的模式有三种，分别是（）（）和（）。

桥接模式（Bridged）、NAT模式、仅主机模式（Host-Only模式）

7、VMware虚拟机默认有两块虚拟网卡，分别是vmnet1和vmnet8，其中vmnet1对应于（）模式，vmnet8对应于（）模式。

仅主机模式、NAT模式

8、Windows系统中查看本地网络信息的命令是（），Kali系统中查看本地网络信息的命令是（）。

ipconfig、ifconfig

9、Kali系统中启动SSH服务的命令是（）。

service ssh start

10、信息收集是进行安全渗透测试必要的准备工作，其主要目的是收集渗透测试目标的基本信息，包括（）（）和（）。

操作系统信息、网络配置信息、应用服务信息

11、信息收集的目标通常有（）（）（）和（）。

硬件设备、操作系统、应用软件、网络环境

12、按照信息收集的方式来分，信息收集可以分为（）和（）。

被动信息收集、主动信息收集

13、Kali系统查询本机的IP地址的命令是（）。

ifconfig

14、给出三种常见的漏洞扫描工具（）（）和（）。

Nmap、Nessus、OpenVAS

15、Payload模块也称攻击载荷，其有三种类型，分别是（）（）和（）。

独立攻击载荷、传输器载荷、传输体载荷

16、MSF框架中的渗透攻击模块按照可以利用的安全漏洞位置分为（）和（）两类。

主动渗透攻击、被动渗透攻击

17、密码技术有三项核心的功能：（）（）和（）。

加密、身份认证、完整性验证

18、创建密码字典的工具有（）和（）。

Crunch、retgen

19、权限提升的方式主要有（）和（）。

模拟令牌、社会工程工具包

20、Windows系统有两种类型的访问令牌：（）和（）。

主令牌、模拟令牌

21、目前无线网络的接入方式主要有两种：（）和（）。

数字蜂窝接入、无线局域网接入

22、WLAN有两种不同的体系结构，分别是（）和（）。

基础结构网络（infrastructure网络）、自组织网络（Ad Hoc网络）

23、Kali系统中启动Web服务的命令是（）。

service apache2 start

# 三、判断（5\*2）

1、Nessus是一种漏洞扫描工具，它是完全免费的。

×

2、主动渗透攻击针对的是服务器端，被动渗透攻击针对的是客户端。

√

3、Windows系统中一个正模拟客户端的线程拥有一个主令牌和一个模拟令牌。

√

4、Windows系统中每一个进程有一个主令牌和一个模拟令牌。

×

5、DVWA是一个Web漏洞演练平台，是PHP编写的。

√

6、无线网络除了链路层与有线网络不同外，其他没有本质的区别，都基于TCP/IP协议栈。

√

7、无线网络与有线网络采用的传输链路完全不同，因此有线网络中存在的安全问题并不适用于无线网络。

×

8、基础结构无线网络就是基带站（即无线接入点）的无线网络。

√

9、自组织网络是一种多跳的、无中心的、自组织无线网络，又称为多跳网（Multi-hop Network）、无基础设施网（infrastructuress Network）或自组织网（Self-or-ganizing Network）。

√

10、Airodump-ng可用于伪造AP接入点。

×

# 四、名词解释（5\*5）

1、黑盒测试

黑盒测试是在对基础设施不知情的情况下进行测试

2、白盒测试

白盒测试是在完整了解结构的情况下进行测试

3、灰盒测试

介于黑盒测试与白盒测试之间，是较为隐秘地进行测试

4、数字取证

数字取证主要是针对各种电子证据进行识别、收集、保存和分析，用来发现网络和系统的各种入侵行为，为进一步的安全处理提供依据。

5、安全审计

安全审计是由“专业审计人员根据有关的法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并做出相应评价”。

6、渗透测试

渗透测试是Kali系统最主要的功能，它是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。

7、电子证据

电子证据，是指以存储的电子化信息资料来证明案件真实情况的电子物品或电子记录。

8、靶机

在使用Kali系统进行安全渗透测试时，需要有一个攻击或渗透测试的对象或目标，这就是靶机。靶机可以是一个完整的操作系统或者一个面向特定应用的软件（如Web 应用、邮件应用），在系统和软件上有很多漏洞供用户进行安全渗透测试的试练。

9、被动信息收集

被动信息收集不会与目标服务器做直接的交换，在不被目标系统查觉的情况下，通过搜索引擎、社交媒体等方式对目标外围的信息进行收集。

10、主动信息收集

主动信息收集会与目标系统有直接的接触和交互，从目标系统直接获取需要的情报信息。

11、旁站查询

所谓旁站就是和目标网站处于同一服务器的站点，通过查询服务获取目标网站的旁站信息。

12、指纹探测

指纹探测就是对目标主机的系统版本、服务版本以及目标站点所用的内容管理系统版本进行探测，为漏洞发现做铺垫。

13、漏洞

漏洞更准确的描述应该是脆弱性，是指在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

14、Payload

Payload又称为攻击载荷，该载荷被渗透攻击模块利用目标主机的安全漏洞植入目标主机中并运行，主要用来在攻击主机与目标主机之间建立一个稳定的连接。

15、主动渗透攻击

主动渗透攻击利用的是位于（服务器端软件和程序）网络服务端软件以及服务所承载的上层应用程序中存在的安全漏洞，主动直接连接服务开放的监听端口，然后注入一些包含恶意请求或代码的内容，触发安全漏洞，进而使得远程服务进程执行恶意代码中包含的攻击载荷，从而获取目标系统的访问控制权。

16、被动渗透攻击

被动渗透攻击利用的则是客户端软件中存在的安全漏洞，如浏览器、电子邮件、Office办公软件等。这些客户端程序没有公开的服务端口供攻击者去连接，只能采用被动渗透攻击方式。

17、密码字典

在密码字典中按照由短到长、由简单到复杂、由常用到不常用的顺序保存的密

码组合，密码破解工具将会按照密码字典中存储的密码顺序去逐一尝试，直到

密码匹配或者密码字典中的密码耗尽为止。

18、密码爆破

“密码爆破”就是通过枚举（穷举）的方式来破解密码。

19、彩虹表

彩虹表是一个散列值的集合，为了破解密码的散列值，人们预先计算各种字母组合的散列值，并将其存储在彩虹表中。

20、模拟令牌

模拟令牌是Windows系统提供的一种访问控制机制，利用这种机制攻击者可以假冒网络中的用户进行各种操作，比如创建用户和组、提升用户权限等。

21、访问令牌

访问令牌是Windows 操作系统安全性的一个概念。当用户登录时，系统创建一个访问令牌，里面包含登录进程返回的SID和由本地安全策略分配给用户和用户的安全组的特权列表。

22、主令牌

主令牌是由Windows 内核创建并分配给进程的默认访问令牌，每一个进程有一个主令牌，它描述了与当前进程相关的用户账户的安全上下文。

23、SQL注入

通过利用一些查询语句的漏洞，将sql语句传递到服务器解析并执行的一种攻击手段。

24、Wardriving入侵

WarDriving也称为接入点映射或驾驶攻击，是一种在驾车围绕企业或住所邻里时扫描无线网络名称的活动。

25、非法AP

非法AP是未经网络管理人员同意或授权的、非法搭建的无线接入点。

# 五、简答题（6\*5）

1、渗透测试的两个主要特点是什么？

渗透测试有两个主要的特点：首先渗透测试是一个渐进的并且逐步深入的过程；其次，渗透测试选择不影响业务系统正常运行的攻击方法进行的测试。

2、VMware虚拟机连网有哪几种方式，这些方式的区别是什么？

VMware虚拟机连接有线网络的模式有三种：桥接模式（Bridged）、NAT模式和仅主机模式（Host-Only模式）。

1）桥接模式下虚拟机与物理机处于同一网段，相当于通过虚拟交换机相连，虚拟机可以通过物理机访问外网。

2）NAT模式下虚拟机在私有网中，与物理机处于不同的网段，虚拟机采用私有IP地址，开启了NAT功能，虚拟机可通过物理机访问外网。

3）仅主机模式下虚拟机与NAT模式下的虚拟机类似，也是位于私有网络，采用私有IP地址，但是没有开启NAT功能，无法访问外网。

3、电脑安装VMware虚拟机后，会看到两块虚拟网卡，这两块虚拟网卡的名字默认是什么？分别对应虚拟机的哪种网络连接方式？

vmnet1和vmnet8，其中vmnet1对应于仅主机模式，vmnet8对应于NAT模式。

4、彩虹表是怎么破解密码的？

彩虹表是一个散列值（也叫哈希值、报文摘要）的集合，为了破解密码的散列值（密码往往以散列值的形式存储），人们预先计算各种字母组合的散列值，并将其存储在彩虹表中。其实字母组合就是密码，彩虹表存储的不是密码本身，而是密码的散列值。在破解密码时，将彩虹表中的散列值与密码的散列值进行比较，同样可以找到密码。

5、什么是C段？

我们知道IPv4地址常用点分十进制表示，每个IP地址都有四个分段，如IP地址“123.125.115.110”，123为A段，125为B段，115为C段，110为D段。

6、在MSF中，渗透攻击模块中的作用是什么？

渗透攻击模块是MSF框架中最为核心的功能组件，它主要利用发现的安全漏洞或配置弱点对远程目标系统进行攻击，以植入和运行攻击载荷，从而获取远程目标主机系统的访问控制权。

7、在MSF中,编码器模块的作用是什么？

在目标系统运行的是攻击载荷模块与空指令模块共同生成的一个带有空指令和Shellcode指令的序列，但是这样的指令序列多数情况下并不能直接在目标系统上运行，需要进行编码，否则很可能无法正常运行或者达不到渗透攻击的效果。

8、在进行漏洞利用时，为什么需要执行一些空指令？

空指令是一些对程序运行状态不会造成任何实质性影响的空操作或无关操作的指令，其作用是为了填充数据的需要。在多数情况下，需要在真正要执行的Shellcode代码之前需要填充一些毫无意义的空指令，从而避免由于内存地址随机化、代码执行地址计算偏差、代码返回地址计算偏差等因素导致Shellcode运行失败，从而可以提高渗透攻击的有效性。

9、简述用Meterpreter建立会话的一般步骤。

1）生成后门程序文件

2）将后门程序上传到靶机并添加可执行权限

3）启动MSFConsole并使用“exploit/multi/hander”模块开始监听

4）在靶机上运行后门程序

5）获取反向连接shell并运行meterpreter

10、用Burp Suite对DVWA的登录账号和密码进行暴力破解时，需要怎样设置才能让Burp Suite拦截浏览器发往DVWA的网页请求？

1）首先要开启Burp Suite的代理功能，将其作为浏览器上网的代理，需要设置IP地址和端口号。

2）需要在浏览器设置代理，在浏览器的连接中，将其上网方式改成通过代理上网，并将代理服务器的IP地址和端口号设置为Burp Suite代理功能设置的IP地址和端口号。

11、简述用Burp Suite对DVWA的登录账号和密码进行破解的一般步骤。

1）将DVWA的安全等级设置为低

2）启动并初始化Burp Suite

3）Burp Suite服务代理设置

4）浏览器代理设置

5）破解DVWA登陆页面：开启Burp Suite拦截功能，浏览器登录，拦截浏览器发往DVWA服务器的网页后，选定要被破解的对象账号和密码，加载相应的字典文件，开始破解，Burp Suite会自动用字典文件中的账号和密码进行登陆尝试，数据包长度与其他数据包长度差异明显的即为破解的账号和密码。

12、非法AP危害很大，它有那些形式？

非法AP有两种形式，一是利用专用软件将计算机伪装成AP。这种方式具有很强的破坏性，可以实施中间人攻击，对授权客户端和AP进行双重欺骗，进而对信息进行窃取和篡改。二是利用真实的AP,非法放置在被入侵的网络中，来窃取无线客户端的信息。

13、非法AP对WLAN有哪些危害？

非法AP对WLAN的危害很大，主要表现在以下三个方面：

1）占用正常信道，干扰正常的无线通信；

2）截取无线网络通信信号，入侵个人计算机，造成个人信息的泄露；

3）如果是在企事业单位内部网络上搭建非法AP，则会严重威胁内网安全。

14、Kali虚拟机如何进行连接无线网络，从而对无线网络进行渗透测试？

Kali虚拟机需要通过无线连接网络，常用的方法是物理机连接一块基于USB接口的无线网卡,VMware虚拟机工具会将该无线网卡映射到虚拟机操作系统上，这样虚拟机操作系统就可以通过无线网卡访问网络了。

15、小米随身WIFI有哪些主要功能？

小米随身WIFI是北京小米科技有限责任公司的一块产品，该产品主要有两大功能：

1）无线网卡功能：无法连接无线的台式电脑或无自带网卡的笔记本，只要插入随身WIFI，切换至无线网卡模式，即可接收WIFI信号；

2）随身WIFI功能：将小米随身WIFI插上一台已上网的电脑，小米随身wifi就创建免费WIFI网络，让用户的手机和平板立刻连上WIFI。

16

