第一部分：判断题

1. 基本的网络测试命令有：ping、tracert、show、debug 命令等。(错)
2. 在 Windows 系统的域中，更新组策略的命令为 gpupdate.exe。(对)
3. 通过命令 arp -s 可以手动加入一条错误的地址缓存来实现临时阻止某台计算机对你的访问。(对)
4. 在设置防火墙规则时可以对端口范围进行自定义。(对)
5. 在一个局域网中，可以同时建立多个工作组，它们的名称可以相同。(错)
6. 假设一个工作组中有 100 台计算机，如果一个用户需要访问每台计算机上的资源，那么只需要在工作组中为他创建一个用户账号即可。(错)
7. 如果 PC(Windows 操作系统)的 DHCP 客户端无法获得 IP 地址，将从 Microsoft 保留地址段 169.254.0.1~169.254.255.254 中选择一个作为自己的地址。(对)
8. Windows Server 的动态卷一共有 3 中类型，包括简单卷、跨区卷、带区卷。(错)
9. Windows 防火墙是一个基于主机状态的防火墙，只丢弃所有未经请求的传入流量。(对)
10. TCP 端口范围是 0-65536，一般使用 1024 以上的端口。(对)
11. Chroot 方式部署的 DNS 服务比常规方式部署的 DNS 服务安全性更高。(对)
12. Windows Server 2008 中的本地账户可以登录到域中，并可以获得该网络中任意一台机器的登录权限。(错)
13. 封堵 445 端口、禁用 SMB 服务可以防御永恒之蓝加密勒索病毒的传播。(对)
14. 通过大量伪造的 ICMP 请求和 UDP 请求导致系统变卡顿甚至重新启动，这种攻击我们称之为逻辑炸弹。(错)
15. 域账号的名称在域中必须是唯一的，而且也不能和本地账号名称相同。(对)
16. Windows 防火墙能够帮助检测和清除已经感染计算机的病毒和蠕虫。(错)
17. Telnet 服务自身的主要缺陷是明文传输用户名和密码。(对)
18. 在我国严重的网络犯罪行为不需要接受刑法的相关处罚。(错)
19. Kerberos 协议是建立在非对称加密算法 RSA 上的。(错)
20. IPSec 协议是运行在应用层上的协议，SSL 协议是运行在网络层上的协议。(错)
21. SYN Flood 利用的是 TCP 连接三次握手的弱点进行攻击的。(对)
22. Kerberos 是对称密钥，PKI 是非对称密钥。(对)
23. 在 Windows 2000/XP/03 中，开始/运行：gpupdate 可以打开“本地策略编辑器”的管理控制台。(错)

24. 一台服务器对网络的响应速度变得很慢以致没有响应。使用 Wireshark 抓包发现该电脑每秒接收到数百万个 ICMP 数据包。由此判断该服务器遭受了 DDOS 攻击。(对)
25. Kerberos 服务是单点登录系统，对于每次会话都需要向 Kerberos 服务进行验证，保护该会话过程中所有后续事务的安全。(错)

第二部分：多选题

1. 关于 OpenSSH 服务的作用描述正确的是：(A、C)
- A、OpenSSH 服务是开放源代码的安全加密程序；B、OpenSSH 服务常用于为 HTTP 协议加密；C、OpenSSH 服务用于提高远程登录访问的安全性；D、OpenSSH 和 Telnet 服务使用同样的端口号
2. 在某浏览器中访问 <https://www.pyseclabs.com> 时，弹出如下图所示的对话框，从附件中的图片可以得知 (A、C)。
- A、访问的站点启用了 SSL；B、该站点要求客户端必须有证书；C、站点的证书是由该浏览器不信任的 CA 颁发；D、该站点安装的证书包含网站的 FQDN: www.pyseclabs.com
3. 局域网中有一台 Windows Server 2008 的 Web 服务器只有一个 IP 地址，使用 (C、D) 方式可以在该服务器上利用 IIS 搭建两个网站。
- A、相同的 IP 地址和不同的默认文档；B、相同的 IP 地址和不同的 UDP 端口；C、相同的 IP 地址和不同的 TCP 端口；D、相同的 IP 地址、TCP 端口和不同的主机头
4. 下列关于防火墙的维护和策略制定说法正确的是：(A、B、C、D)。
- A、对防火墙策略进行验证的方法是：通过在防火墙规则影响的主机上测试指定服务的连通性来进行验证；B、所有防火墙管理功能应该发生在使用了强认证和加密的安全链路上，从而避免防火墙策略被泄露的威胁；C、在对防火墙进行远程管理时，使用 timeout 选项是一种较为稳妥的做法，尤其是在测试更复杂的规则集时，若规则没有按预期运行，甚至可能将管理员锁定而使其无法进入系统，那么规则将被自动删除；D、在测试新的且带有一定危险性的防火墙策略时，管理员可以通过省略 --permanent 选项，以临时来运行防火墙配置
5. 关于如何修复 MS08_067 漏洞，说法正确的是：(A、B、C、E)。
- A、安装电脑管家，进行系统补丁修补；B、停用文件共享服务，关闭 139、445 端口；C、开启防火墙阻止 135、139、445 等端口的流量传入；D、使用 Ghost 版的 Windows

XP 重新安装系统； E、停用当前版本的操作系统，通过国内运营商购买 Windows 10 密钥，并通过微软官网下载安装最新版的 Windows 10 操作系统镜像并安装。

6. 使用 Metasploit 中的 exploit/multi/handler 模块对反弹型木马进行监听，以下参数描述正确的是：(B、C)。

A、REMOTE_ADDR – 设置目标主机地址； B、LHOST – 设置本地地址； C、LPORT – 设置本地监听端口； D、RHOST – 设置本地地址。

7. 2017 年 5 月，全球十几万电脑收到勒索病毒 WannaCry 攻击，电脑被感染后文件会被加密锁定，从而勒索钱财。在应对该病毒时，安全人员应该如何预防这一类型的攻击 (A、C、D)。

A、删除可疑的邮件，尤其包含连接或附件的； B、安装 Ubuntu 和 Windows 双系统可以免受勒索病毒的攻击； C、定期备份电脑上的档案至云服务器，确保电脑上的入侵防护软件更新至最新的版本，保持更新操作系统及其他软件的习惯； D、一旦受到感染，马上将受感染的电脑从网络上及外置存储设备装置隔离。

8. 关于 WannaCry 勒索病毒，下列描述错误的是：(A、B)。

A、可以随意下载并打开邮件中的附件； B、只安装杀毒软件就可以让电脑不受黑客和病毒的入侵； C、一旦受到感染，马上将受感染的电脑从网络上及外置存储设备装置隔离； D、定期更新系统补丁并安装杀毒软件，可以提高计算机的安全性。

9. 下列关于协议描述正确的是：(B、C、D)。

A、SSH 协议专为远程登录会话和其他网络服务提供安全性的认证服务； B、SSL 协议为数据通信提供安全支持； C、TLS 协议用于在两个通信应用程序之间提供保密性和数据完整性； D、IPSec 协议通过使用加密的安全服务以确保网络上进行安全的通信。

10. 使用 Nmap 扫描工具能够 (A、B、C、D)。

A、判断操作系统类型； B、确认开放的端口； C、识别网络的拓扑结构； D、测试系统是否存在安全漏洞； E、识别出入侵者的行为

11. 仔细阅读以下 DHCP 客户端租约文件，如果该 DHCP 服务器在国内，以下说法正确的是：(A、B、D)。

A、客户端所分配到的 IP 地址为 172.16.1.128； B、/var/lib/dhcpd/dhcpd.leases 这个文件专门记录了 DHCP 的分配情况； C、客户端的网卡 MAC 地址是由 DHCP 服务分配的； D、租约数据库文件中使用的是格林威治标准时间； E、租约到期时间为北京时间 2020 年 3 月 28 日 8 点 43 分 58 秒

12. Windows Server 2003 系统中 IIS 6.0 服务的主要安全缺陷表现在攻击者可以：(A、B、C)。
- A、利用 HTTP 协议进行的拒绝服务攻击； B、利用 IIS 6.0 版本中的 WebDAV 服务的“ScStoragePathFromUrl”函数存在缓冲区溢出漏洞； C、利用 IIS 6.0 解析漏洞上传木马，获得网站权限； D、利用 MDAC 组件的漏洞进行远程代码执行；
13. 在 CentOS 7 系统中，已安装了 VsFTPd 服务，在 /var/ftp 目录下创建了一个权限为 777 的 anon 文件夹，关闭 selinux，在默认配置的情况下，要设置允许匿名用户可在 anon 文件夹中上传文件，至少要在 vsftpd.conf 文件中添加 (A、C、E) 配置参数。
- A 、 anonymous_enable=YES ; B 、 anon_mkdir_write_enable=YES ; C 、 anon_upload_enable=YES; D、upload_enable=YES; E、anon_other_write_enable=YES
14. VSFTPD 服务提供了灵活的访问控制设置方法，可以通过修改配置文件的选项实现允许或拒绝访问 FTP 服务器的用户账号，当只允许/etc/vsftpd/user_list 文件中的用户登录 vsftpd 服务器时，在 vsftpd.conf 配置文件中应同时设置：(A、C、D)。
- A、userlist_enable=YES; B、userlist_deny=YES; C、local_enable=YES; D、userlist_deny=NO;
15. 某公司的网络管理员小王需要在他的个人 Linux 服务器上，通过 NFS 访问公司的文件服务器 nfserver 上的资源，公司的服务器通过 CentOS7 和 NFS 部署了文件服务器，使用的共享目录位于 /home/nfsdir。他执行哪些命令可以挂载共享目录：(A、D、E)
- A、使用命令 `mount -t nfs nfserver:/home/nfsdir /mnt/nfs`； B、使用命令 `mount nfs://nfserver/home/nfsdir /mnt/nfs`； C、使用命令 `mount -t nfs //nfserver/home/nfsdir /mnt/nfs`； D、使用命令 `echo "nfserver:/home/nfsdir /mnt/nfs nfs defaults 0 0" >> /etc/fstab`，然后使用命令 `reboot`； E、使用命令 `echo "nfserver:/home/nfsdir /mnt/nfs nfs defaults 0 0" >> /etc/fstab`，然后使用命令 `mount -a`。
16. 网关服务器外网口 IP 地址为 172.16.1.200/24，内网口 IP 地址为 192.168.2.1/24，默认开启路由转发功能，内网 Web 服务器 IP 地址为 192.168.2.200/24，已配置网关的地址为 192.168.2.1/24，在防火墙默认阻止所有流量传入的前提下，以下哪些命令能使外部网络可以浏览内部网络的网站：(B、D)
- A、`iptables -t nat -A PREROUTING -i eth0 -p tcp -d 172.16.1.200 --dport 443 -j DNAT`

--to-destination 192.168.2.200:443; B、iptables -A INPUT -i eth0 -p tcp -s any/0 --sport 1024:65535 -d 172.16.1.200 --dport 443 -j ACCEPT; C、firewall-cmd --add-rich='rule family=ipv4 source address=172.16.1.0/24 masquerade'; D、firewall-cmd --permanent --add-rich-rule='rule family=ipv4 destination address=172.16.1.200/32 forward-port port=443 protocol=tcp to-addr=192.168.2.200'。

17. Rsyslog 日志级别都有哪些：(A、B、C、D)。

A、debug; B、info; C、notice; D、warning; E、news。

18. 附件中的截图是 Rsyslog 日志服务器的配置文件截图，下列说法正确的是：(A、B、D、E)。

A、Rsyslog 日志服务器监听的端口为 514 号，协议是 UDP; B、Rsyslog 允许从 172.16.1.0/24 网段的主机发送日志文件到该服务器中; C、该日志服务器采集所有的日志信息包括本机; D、日志文件存放的路径位于：/var/log/remote/发送日志的 IP 地址/年~月~日; E、欲接受内网主机发送过来的日志文件需在防火墙规则中放行从 514 号端口传入的 UDP 数据。

19. 防范或缓解 ARP 欺骗攻击的主要方法有：(A、B、C)。

A、在交换机上配置 VLAN 来隔离广播域缩小感染的范围; B、利用 NBTScan 工具查出局域网中 IP 对应的 MAC 地址并手动建立 ARP 数据库，然后添加静态的 ARP 缓存，在各主机上将网关的 IP 和 MAC 进行绑定; C、部署支持 ARP 过滤的防火墙，动态的监测局域网内针对本主机和针对网关的 ARP 欺骗; D、使用命令 arp -d 删除所有 ARP 缓存信息，等待 ARP 缓存表更新;

20. 以下有关 P0f 工具的描述正确的是：(B、C)。

A、参数“-o file”为指定指纹数据库的路径，不指定则使用默认数据库 (/etc/p0f/p0f.fp); B、参数“-i iface”为指定要监听的网络接口; C、参数“-p”将监听的网卡设置为混杂模式; D、参数“-f file”指定读取有抓包工具抓到的网络数据包文件; E、参数“-d”的作用是以后台进程方式允许 p0f。

21. iptables 与 firewall 的区别说法正确的是：(A、B、D)。

A、iptables 通过控制端口来控制服务，而 firewalld 则是通过控制协议来控制端口; B、iptables 是一个命令行的防火墙管理工具，真正的防火墙是内核中的 netfilter 网络过滤器; C、iptables 用于过滤数据包，不属于网络层防火墙; D、firewalld 防火墙有两种管理方式，firewall-cmd 和 firewall-config。

22. 下列哪些工具可以用来抓取 Windows 内存中的明文密码。(A、C)。

A、WCE; B、CAIN; C、Mimikatz; D、Quarks PWdump。

23. TCPDump 是一个运行在命令行下的嗅探工具。以下关于 TCPDump 参数描述正确是：

(A、B、D)。

A、参数“-i”指定 tcpdump 需要监听的接口。如果没有指定，tcpdump 会从系统接口列表中搜寻编号最小的已配置好的接口；B、参数“-C”的作用是在将一个原始分组写入文件之前，检查文件当前的大小是否超过了参数 file_size 中指定的大小。如果超过了指定大小，则关闭当前文件，然后在打开一个新的文件；C、使用命令 tcpdump -i eth0 udp dst port 53 抓取网络中所有 DNS 应答的数据；D、使用命令 tcpdump ip host 172.16.1.100 and ! 172.16.1.200 -c 10 -i any 获取主机 172.16.1.100 和除 172.16.1.200 之外所有主机的通信，并只抓取 10 个包。

24. 查看附件中的截图，以下有关 FirewallD 说法正确的有：(A、B、C、D、E)。

A、第一条命令的作用是添加一条链规则为 blacklist 到 raw 表中；B、第二条命令的作用是通过添加直接规则以将来自 172.16.1.0/24 网络的 IP 列入黑名单；C、第三条命令作用是在 raw 表中指定 blacklist 链添加规则：单个 IP 每分钟并发量为 1,并生成一个日志文件，日志文件的前缀为 blacklisted；D、第四条命令的作用是将来自 172.16.2.0/24 的主机访问 5432 号端口的流量转发到 22 号端口，并记录日志，日志前缀为[ADMIN LOGIN]，而且限制每分钟只记录一条日志；E、第五条命令的作用是将来自规则链“blacklist”中的数据包丢弃。

25. DHCP 可以提供的服务包括 (A、C、D)。

A、为特定客户机提供固定 IP 地址服务；B、为主机设置防火墙；C、提供动态主机地址分配；D、分配 DNS、网关等方面的基本网络信息。

第三部分：单选题

1. 渗透测试人员常用 Nmap 工具进行网络连通性测试，参数-sP 的工作原理为：(B)
A、向目标主机发送 UDP Echo Request 数据包，等待对方回应 UDP Echo Reply 数据包；
B、向目标主机发送 ICMP Echo Request 数据包，等待对方回应 ICMP Echo Reply 数据包；
C、向目标主机发送 UDP Echo Reply 数据包，等待对方回应 ICMP Echo Request 数据包；
D、向目标主机发送 ICMP Echo Reply 数据包，等待对方回应 ICMP Echo Request 数据包
2. 某公司 Linux 主机被恶意用户进行了 SSH 密码暴力枚举，此时网络管理员需要拒绝其访问的源 IP，应该采取下列哪种方式查询其访问的记录？(A)。
A、cat /var/log/secure； B、cat /var/audit/audit.log； C、cat /etc/security/access.log；
D、cat /var/log/messages
3. 某公司的计算机处在单域的环境中，有 10 台服务器运行了 Windows Server 2008，另外的 30 台 PC 是运行的 Windows 10。有员工反馈，在登录和访问服务器时，经常出现“由于时间差异，访问被拒绝”的提示，为了解决这一问题，应该查看(C)是否工作正常，并重启客户机的 Windows Time 服务。
A、Task Scheduler 计划任务服务； B、Kerberos 身份验证服务； C、Active Directory 域服务； D、Domain Name Server 域名服务
4. 某公司在 Windows Server 2008 服务器上搭建了 DHCP 服务，由于 RAID 卡故障，导致服务器宕机。此时最佳的恢复 DHCP 服务的方式是：(B)。
A、将其他计算机上的网络操作系统全盘拷贝至宕机的服务器上，然后重新安装 DHCP 服务；
B、使用硬盘中保存完好的 DHCP 数据库备份信息在另一台服务器上恢复服务；
C、通过安全模式进入操作系统中，然后启动 DHCP 服务继续提供服务；
D、等待 RAID 卡生产商技术人员更换新的硬件，然后重新安装操作系统和 DHCP 服务
5. 管理员小王在 Windows Server 2008 服务器上部署了远程访问服务，可是小王在测试过程中发现通过 VPN 进行远程连接之后发现，他只能通过内网地址访问远程服务器，无法访问服务器中的其他主机，可能的原因是：(B)。
A、小王获取到的内网 IP 不正确或未正确配置 VPN；
B、在远程访问服务器属性的 IPv4 选项卡中没有选择“启用 IPv4 转发”；
C、远程访问服务器所配置的身份验证方法拒绝了小明的连接请求；
D、远程访问服务器拒绝了小王所在的局域网中的主机访问。
6. 合理的使用 IIS7.0 当中的虚拟目录功能可以提高工作效率。下面关于虚拟目录描述错误

的是：(C)。

A、使用虚拟目录可以将数据分散保存到不同的磁盘或计算机上，便于开发与维护；B、WWW 服务和 FTP 服务都支持虚拟目录功能；C、虚拟目录和物理目录是紧密相关的。在 IIS 上删除虚拟目录后，物理目录也会被删除；D、当硬盘中的数据移动到其他物理位置时，不会影响到 Web 站点的逻辑结构。

7. 以下为 DHCP 协议交互过程中的四种消息，正确的顺序应该是：(B) ①DHCP Ack ②DHCP Discovery ③DHCP Offer ④DHCP Request。

A、①③②④；B、②③④①；C、②①④③；D、②④③①。

8. 某公司有一台 Linux 服务器，网络管理员在服务器上部署了 DHCPD 服务，附件中的截图为该服务的配置文件，有关配置文件描述正确的是：(C)。

A、配置文件中的 default-lease-time 表明客户端 IP 地址的缺省租用期为 12 小时；B、配置文件中的 option time-offset 表明设置时间（与北京时间）偏差为 5 小时；C、配置文件中的 option time-offset 表明设置时间（与格林威治时间）偏差为 5 小时；D、配置文件中的 max-lease-time 表明客户端 IP 地址的最大租用期为 6 小时。

9. 渗透测试人员通过对目标主机进行端口扫描可直接获得：(D)。

A、目标主机的操作系统信息；B、目标主机的登录口令；C、目标主机的硬件设备信息；D、目标主机端口的状态信息。

10. SSL 产生会话密钥的方式是：(D)。

A、由服务器产生并分配给客户机；B、每一台客户机分配一个密钥；C、从密钥管理数据库中请求获得；D、由客户机随机产生并加密后通知服务器

11. 以下哪个工具是 Nmap 的图形化界面版：(B)。

A、Sqlmap；B、Zenmap；C、Zamp；D、Gnmap

12. VPN 使用了 () 技术保证了通信的安全性：(D)。

A、隧道协议、数据加密；B、隧道协议、身份认证；C、身份认证、数据加密；D、隧道协议、身份认证和数据加密；

13. 关于组策略的处理规则，描述不正确的是：(C)。

A、系统是先处理计算机配置，再处理用户配置；B、组策略的配置是有累加性的；C、当计算机组策略设置和用户组策略设置发生冲突时，系统会优先应用用户组策略；D、如果子容器内的某个策略被配置，则此配置值会覆盖由其父容器所传递下来的配置值

14. 小王是某公司的网络管理员，公司的计算机处于单域中，他使用的操作系统为 Windows Server 2012, 由于计算机中有非常重要的资料，因此他想设置一个安全的密码。下面 (C) 是比较安全的密码。

A、138*****; B、将操作系统管理员账号的口令设置为空; C、QvDa!3@#*&*(L2i; D、xiaowang2020;

15. 假设你是某公司网络管理员，出于安全性的考虑，你希望使用这台计算机的用户账号在更改密码时不能用前两次用过的密码，应该采取的措施是：(C)

A、制定一个行政规定，要求用户不得使用前 2 次的密码; B、设置计算机本地安全策略中的密码策略，设置“密码最长存留期”的值为 2; C、设置计算机本地安全策略中的安全策略，设置“强制密码历史”的值为 2; D、设置计算机本地安全策略中的密码策略，设置“账户锁定时间”的值为 2

16. 假设你是某公司的网络管理员，公司处在单域的环境中且有两个部门：市场部和技术部，每个部门在活动目录中有一个相应的 OU(Organization Unit 组织单位),分别是 MARKET 和 TECHNOLOGY。有一个用户 JACK 要从技术部调动到市场部工作。JACK 的账户原来存放在组织单位 TECHNOLOGY 里，现在需要将 JACK 的账户存放到组织单位 MARKET 里，应该通过 (B) 来实现此功能。

A、将 JACK 使用的计算机重新加入域; B、复制 JACK 使用的账户到组织单位 MARKET 里，然后将 TECHNOLOGY 里的账户删除; C、在组织单位 TECHNOLOGY 里将 JACK 的账户删除，然后在组织单位 MARKET 里新建; D、将 JACK 的账户拖动到组织单位 MARKET。

17. 仔细观察附件中的图片，下列有关 firewalld 防火墙说法正确的是：(C)。

A、为实现内网用户访问互联网，管理员需要在网站服务器上配置地址伪装，使用命令 `firewall-cmd --zone=trusted --add-rich='rule family=ipv4 source address=192.168.2.0/24 masquerade'`; B、为实现内网用户访问互联网，管理员需要在网关服务器上配置地址伪装，使用命令 `firewall-cmd --zone=external --add-rich='rule family=ipv4 destination address=192.168.2.0/24 masquerade'`; C、为实现互联网用户访问内部 Web 服务器，管理员需要在网关服务器上配置端口转发，使用命令 `firewall-cmd --zone=external --permanent --add-rich-rule='rule family=ipv4 destination address=172.16.1.200/32 forward-port port=443 protocol=tcp to-addr=192.168.2.200'`;

D、为实现互联网用户访问内部 Web 服务器，管理员需要在网站服务器上配置端口转发，使用命令 `firewall-cmd --zone=external --permanent --add-rich-rule='rule family=ipv4 destination address=192.168.2.200/32 forward-port port=443 protocol=tcp to-addr=172.16.1.200'`。

18. 中间人攻击就是在通信双方毫无察觉的情况下，通过拦截正常的网络通信数据，进而对数据进行嗅探或篡改。以下属于中间人攻击的是：（ B ）。

A、隧道加密技术； B、社会工程钓鱼攻击； C、分布式拒绝服务攻击； D、OpenSSL 心脏滴血。

19. 小王在一家公司中担任网络管理员，公司的网络中利用 DNS 实现域名解析服务，现准备对其进行整改在网络中添加 Web 服务器向其他计算机提供 Web 浏览服务。但由于需要 Web 服务的访问量巨大，所以为了提供较好的服务，小王将三台具有相同主机名的 Web 服务器做一个集群。为了让这三台服务器能够随机的用户访问请求作出响应，小王在 DNS 服务器上为同一个主机名创建了三条主机记录，分别对应这三台 Web 服务器的 IP 地址。改造完成后小王利用监视器对三台 Web 服务器进行监视时发现，实际只有一台 Web 服务器能够对用户的请求进行响应，应采取何种措施以使这三台 Web 服务器都能够对用户的请求进行响应以提高服务能力？（ C ）。

A、为这三台 Web 服务器指定不同的主机名； B、将这三台 Web 服务器作为 DNS 服务器的客户端； C、在 DNS 服务器上启用转发功能； D、在客户端利用 IP 地址指定 Web 服务器；

20. 关于域组的概念，下列描述正确的是：（ C ）。

A、全局组只能将同一域内用户加入到全局组； B、域本地组的用户可以访问所有域的资源； C、通用组可以包含域本地组； D、域本地组可以包含其他域的域本地组。

21. 使用 Nmap 工具想要探测 1-65535 端口运行的服务版本信息需要使用（ C ）参数。

A、`-v -sS -T4`； B、`-v -sP`； C、`-sV -p-`； D、`-sS -P0 -A -v`。

22. 小王是一家网络公司的网络管理员，工作职责之一就是负责维护文件服务器。他想审核 Windows Server 2008 服务上的共享 word 文件被删除的情况，需要启动审核策略的：（ ）。

A、审核策略更改； B、审核对象访问； C、审核过程跟踪； D、审核登录事件。

23. 附件中的截图为主机 192.168.23.1 收到 DOS 攻击时，使用命令 `netstat -an` 查看连接数的截图，当时该主机正受到（ A ）类型的 DOS 攻击。

A、SYN FLOOD; B、连接耗尽; C、UDP FLOOD; D、CC。

24. 仔细观察附件中的图片，下列有关 Wireshark 的描述，正确的是：(C)。

A、根据所抓包的内容可以知道上面的蓝色字体为客户端请求的报文，红色字体为服务器回应的报文; B、图片中的会话是通过“追踪流”——“TLS 流”所得到的; C、在过滤器中使用过滤规则：`http.request.method==GET` 可以过滤出客户端发送的 GET 请求数据包; D、在过滤器中使用过滤规则：`src host 172.16.1.200 || http` 即可得到图片中的会话流。

25. MS12-020 及 MS15-034 可以达到的攻击效果为：(A)。

A、造成 Windows Server 2008 操作系统蓝屏重启; B、拿到 Webshell; C、获取数据库信息; D、泄露用户敏感数据。

26. 在 DNS 中“A”记录是用来做什么的：(A)

A、将域名映射为 IP 地址的记录; B、为了创建别名的; C、用于反向地址解析的关键记录; D、将 IP 地址映射为域名的记录

27. 小王要在一台 Windows Server 2008 上利用 Internet Information Service 实现网页浏览服务，小王创建了一个 Web 站点并指定了一个主页文件 Welcome.htm，将其放到 Web 站点的主目录下，当你启动 Web 站点后利用 IE 浏览器访问站点时提示无法显示主页。应采取何种措施以解决这个问题？(D)。

A、重新启动 Web 服务器; B、在 IE 浏览器上指定 Web 站点的服务端口 80; C、在 Web 浏览器中注册网站浏览器证书; D、在 Web 服务器先停止 Web 站点，然后在站点属性页文档标签上手动添加文档 Welcome.htm 并将其移至最高位置，最后重新启动站点

28. 有一台操作系统为 Windows Server 2008 的文件服务器，在此服务器中有一个共享文件夹 Sharefile，用户小王对该文件夹的 NTFS 权限为读取，而共享权限被设置为完全控制，当小王从网络中访问该文件夹时，那么当前他有效的权限是：(B)。

A、完全控制; B、读取; C、更改; D、拒绝访问

29. Wireshark 的 Capture Filter 过滤器中输入过滤条件，通过下列的哪一个过滤条件可以过滤出源地址是 192.168.1.1 的数据包：(D)。

A、`src net 192.168.1.1/24`; B、`ether host 192.168.1.1`; C、`ip.addr == 192.168.1.1`; D、`src host 192.168.1.1`

30. Windows Server 2008 的 NTFS 文件系统具有对文件和文件夹加密的特性。域用户 user1 加密了自己的一个文本文件 jiami.txt。他没有给域用户 user2 授权访问该文件。下面描

述正确的是：(B)。

A、user1 需要解密文件 jiami.txt 才能读取；B、对文件加密后可以预防非授权用户访问，所以 user2 不能读取该文件；C、user2 如果对文件 jiami.txt 具有 NTFS 完全控制权限，就可以读取该文件；D、如果 user1 将该文件 jiami.txt 拷贝到 FAT32 分区上，加密特性不会丢失。

31. 下列关于用户口令说法错误的是：(A)。

A、复杂口令安全性足够高，不需要定期修改；B、口令长度越长，安全性越高；C、口令不能设置为空；D、口令认证是最常见的认证机制。

32. 仔细观察下面的截图，下列描述正确的是：(D)。

A、IP 地址为 172.16.1.50 的服务器正遭受 DDoS 攻击；B、IP 地址为 172.16.1.100 的主机正在对 FTP 服务器实施密码暴力枚举的操作；C、使用 dsniff 软件可以无需任何操作即可嗅探内网中所有认证服务的登录账户及口令；D、参数 -i 为指定要嗅探的网络接口，参数 -t 为加载一个要监听密码的网络服务，服务可以是 FTP、Telnet、HTTP、POP、SNMP 等。

33. 小王在 Windows Server 2008 服务器中通过 Internet 信息服务管理器搭建了一个 Web 站点，并在默认站点下创建了一个虚拟目录 Development，经测试可以成功访问测试页面的内容，由于新业务的需要，欲将虚拟目录中的内容转移到一个新的分区中，管理员(C)能让用户继续使用原来的端口和地址访问网页的内容。

A、更改服务的 TCP 端口号；B、添加一个新的站点，并将路径修改为转移后的文件夹路径；C、将原来虚拟目录的路径修改为转移后的文件夹路径；D、无需任何操作，重启服务器即可。

34. Kerberos 认证方式是基于()体系的可信第三方鉴别协议，负责在网络中进行仲裁及会话密钥的分配：(B)。

A、非对称密钥；B、对称密钥；C、公钥或者私钥；D、非对称密钥和对称密钥组合。

35. 下面说法不正确的是：(B)。

A、IIS 信息服务器管理器上能够同时部署两个端口相同，IP 不同的站点；B、IIS 信息管理服务器支持 UNIX、Linux、Windows 等操作系统；C、使用主机名定义站点后不能设置此站点的端口号；D、IIS 信息服务器上部署的站点可以自定义默认文档

36. 在使用 TCPDump 进行监听时，应将网卡设置成以下哪种监听模式：(D)。

A、单播模式 (Unicast mode)；B、广播模式 (Broadcast mode)；C、组播模式 (Multicast

mode); D、混杂模式 (Promiscuous mode)

37. 在 Linux 中 umask 值为 0022, 那么它所对应的默认文件和文件夹创建的缺省权限分别为以下哪个值: (C)。

A、文件的权限为 644, 文件夹的权限为 744; B、文件的权限为 744, 文件夹的权限为 655; C、文件的权限为 644, 文件夹的权限为 755; D、文件的权限为 755, 文件夹的权限为 644;

38. 小王是某公司的网络管理员, 他长期维护公司中所有的 Windows Server 2008 服务器, 其中一台服务器中搭建了域环境。在此域服务器上部署了共享文件夹 WorkDocument, 小王在此服务器中启用了“审核对象访问”, 他希望通过事件查看器中记录所有登录失败的事件, 但经过了一系列的测试后发现, 即使登录失败了, 在事件查看器中也没有关于失败访问的事件, 可能导致记录失败的原因是: (C)。

A、审核对象访问只能记录成功访问的事件, 而不能记录失败访问的事件; B、审核对象访问只能审核本地访问的失败事件, 而不能记录内网其他机器访问事件; C、小王在域控制器安全策略上没有为 WorkDocument 文件夹上添加用户的详细审核项目; D、小王在域控制器安全策略上启用了审核, 而没有在域安全策略上启用该策略

39. 在 Windows Server 2008 系统中, 为 Web 站点申请并安装了证书, 并在 SSL 设置中勾选“要求 SSL”, 在“客户证书”中选择“必须”, 则下列描述正确的是: (A)。

A、客户端必须申请和安装客户端证书, 例如: “用户”证书; B、客户端必须申请和安装客户端证书, 例如: “Web 服务器”证书; C、无论用户是否拥有证书, 都将被授予访问权限; D、用户可以使用客户端证书访问资源, 但证书并不是必须的;

40. 以下哪个工具使用 Rainbow table(彩虹表)来破解 Windows 的 Hash 密码: (C)

A、Hydra; B、Medusa; C、Ophcrack; D、Cain & Abel

41. 文件传输协议(File Transfer Protocol,简称 FTP 服务)、简单文件传输协议 (Simple Mail Transfer Protocol,简称 SMTP 服务)、超文本传输协议 (Hyper Text Transfer Protocol,简称 HTTP 服务), 以上服务分别对应的端口是: (B)。

A、25 21 80; B、21 25 80; C、21 80 110; D、21 22 25。

42. 在.htaccess 文件中, 将.png 文件当作 PHP 文件解析的语句是 : (B)。

- A、AddHandler php5-script php; B、AddType application/x-httpd-php .png; C、SetHandler application/x-httpd-php; D、AddType application/x-httpd-php .jpg。
43. 永恒之蓝漏洞利用以下哪个端口：(C)。
- A、3389; B、21; C、445; D、3306。
44. 下列哪个属于微软的漏洞公告编号：(C)。
- A、MB17-010; B、KB17-010; C、MS17-010; D、GBT17-010;
45. 以下关于 Metasploit 基本命令的描述，不正确的是：(C)。
- A、msfconsole 命令行下启动 MSF; B、show exploits 显示所有的渗透攻击模块; C、use 搜索某个模块; D、show options 显示模块的参数。
46. Apache 服务器的配置文件 httpd.conf 中有很多内容，以下有关 httpd.conf 配置项描述错误的是：(B)。
- A、在配置项中【AddType application/x-httpd-php .php .php4 .htm .html】，该项的作用是添加可以执行 php 的文件类型，在给定的文件扩展名与特定的内容类型之间建立映射; B、在配置项中【DirectoryIndex default.html default.php index.php index.html】，该项的作用是设置服务器处理未知扩展名的文件类型时，使用的预设格式; C、在配置项中【DocumentRoot "/usr/local/httpd/htdocs"】，该项的作用是指定 Apache 网站默认的根目录; D、在配置项中【MaxKeepAliveRequests 100】，该项的作用是限制每个连接允许的请求数量（当 KeepAlive 启用时），此为 100 个请求。
47. 在 Metasploit v5.0 的 Modules 目录总共有 7 个模块，它们分别为:Auxiliary、Encoders、Exploits、Nops、Payloads、Post 以及 evasion，以下有关 Modules 说法错误的是：(B)。
- A、Auxiliary 模块可以获取目标网段的信息，包括端口开放情况、主机存活情况等信息; B、Exploits 是利用系统漏洞或者缺陷的攻击程序。它们针对特定的操作系统，而且经常是特定的 SP (service pack)，特定的服务，特定的端口，甚至特定的应用程序。它们按操作系统分类，Windows exploits 可以用于 Linux，平台之间是互通的; C、Post 是后渗透测试阶段模块，在获得 meterpreter 的 shell 之后可以使用的各种脚本，比如检查目标系统是不是虚拟机、安装了哪些软件、补丁信息等; D、Payload 是 Metasploit 生成的有效载荷，可以在漏洞利用成功之后附带要执行的文件，可以和 exploit 进行响应交互，通过 Payload 可以实现反弹 shell、bind shell 等。
48. 以下哪款工具对 MS17_010 漏洞进行漏洞验证并获取最高管理员权限：()。
- A、AWVS; B、Nessus; C、Hydra; D、Metasploit。

49. 以下不属于端口扫描技术的是：(C)。

A、TCP Connect; B、TCP FIN; C、TCP No FLAG; D、TCP SYN。

50. 以下哪个是专用于窃听网络中传输口令信息的工具：(C)。

A、PGP; B、Wireshark; C、Dsniff; D、Burpsuite。