网络安全
指南针行动-默写手册

达内网络安全学院

达内·网络安全学院
2023 年 11 月

目 录

达内网络安全学院

##

01.《网络应用基础 - 作者：黄书林》

##

01. 简单描述一下 IP 地址的作用和分类？

1）作用：是用来标识一个网络节点的互联网地址。目前使用的是 IPv4 和 IPv6 二个版本

2）分类：IPv4 地址目前分 ABCDE 五类，范围分别如下：

A 类地址 0~127

B 类地址 128~191

C 类地址 192~223

D 类地址 224~239　　组播地址

E 类地址 240~255　　科研地址

02. 简单描述一下公有地址和私有地址的特点？

公有地址：互联网合法使用，需要向运营商付费申请，可以直接上网通信的地址。全球唯一

私有地址：预留企业内部使用，无需付费，每个人或者公司都能使用，主要解决 IP 地址不足问

题，满足企业内网需求。局域网唯一。

03. 私有 IP 地址的范围？

私有地址范围：

A 类 10.0.0.0-10.255.255.255　　有效主机地址 10.0.0.1-10.255.255.254

B 类 172.16.0.0-172.31.255.255　　有效主机地址 172.16.0.1-172.31.255.254

C 类 192.168.0.0-192.168.255.255　　有效主机地址 192.168.0.1-192.168.255.254

04. 子网掩码的作用？ABC 三类地址的默认子网掩码是？

1）作用：区分 IP 地址的网络位与主机位

2）ABC 类 IP 地址默认子网掩码

A 类 255.0.0.0

B 类 255.255.0.0

C 类 255.255.255.0

05. 什么是网关？相同网段通信需要设置网关地址吗？

网关：从当前网段去往其他网段的出口

相同网络段通信不需要网关

06. 描述修改交换机名为 SW1 的命令

交换机系统视图输入：sysname SW1

07. 为交换机 SW1 设置本地登录密码为 Taren1（用户视图开始）

```
[SW1] user-interface console 0
[SW1-ui-console0] set authentication password cipher Taren1
[SW1-ui-console0] authentication-mode password
```

08. 对真实交换机路由器的管理方法有哪些？分别适合什么环境？

本地：使用 Console 线和设备相连接进行操作，适合新设备调试或者面对面设备调试

远程：开启设备的远程管理功能，通过远程管理软件连接操作，适合线上运行环境调试。

09. VMware 虚拟化里面快照和克隆的特点？

虚拟机快照：

对虚拟机某一时刻的各种数据资料、状态的备份，当虚拟机出现故障以后，可以通过这个快照还原到当初制作快照的状态；可以在虚拟机开机或者关机状态下制作快照；一个虚拟机可以保存多份快照，但是启动虚拟机时同一时刻只能基于其中的一份快照。

虚拟机克隆：

以现有的某一个虚拟机作为模板，生成新的虚拟机的技术；只能在关机状态下制作克隆；可以基于一个虚拟机创建多份克隆，克隆出来的每一个虚拟机可以同时启用。

10. 虚拟机厂商及产品

系 列	PC版	企业版
VMware	VMware Workstation	VMware vSphere
Microsoft	VirtualPC	Hyper-V
RedHat	KVM	RHEV
Oracle	VM VirtualBox	VM Server

11. Windows10 常见版本

家庭版/专业版/企业版/教育版

12. 网络排错常见思路（由近到远）？

先 ping 回环地址 127.0.0.1 --> 检查本机通信，检查网卡本身是否正常

再查看本机 IP --> 确保本机 IP 地址正常

再查看对方 IP --> 确保对方 IP 地址正常

再检查对方防火墙 --> 确保对方防火墙关闭

##

02.《Windows应用安全- 作者：黄书林》

##

01. Windows Server 2016 操作系统的常见版本？

Windows Server 2016 Standard（标准版）
Windows Server 2016 Datacenter（数据中心版）

02. Windows 10 主机如何发起远程桌面连接，远程桌面连接的端口号是多少？

开始-运行-mstsc
远程桌面连接的协议 RDP，端口号为 3389

03. Windows 系统常见内置用户？

Administrator：管理员（权限最大）；
Guest：来宾（权限最小），默认禁用 注：内置用户可以改名和禁用，但无法删除

04. Windows 系统中常见内置组？及作用？

1）Administrators：此组内用户具有系统管理员权限。
2）Users：新用户的默认组
3）Everyone：任何一个用户都属于这个组

05. NTFS 文件系统的特点？

高读写
磁盘空间利用率高（支持压缩、磁盘配额）
安全性高 （支持加密、访问控制）
支持大分区、大文件

06. Windows server 2016 系统中，本地安全策略主要包含？帐户策略主要包含？

1） 本地安全策略主要包含：帐户策略、本地策略
2） 帐户策略主要包含：密码策略、帐户锁定策略

07. 什么样的密码是符合复杂性要求的密码？

英文字母小写、英文字母大写、数字、特殊符号，四个条件取其三

08. 密码长度最小值、最长使用期限、最短使用期限、强制密码历史为 0 分别表示？

密码长度最小值，0 表示无限制；
密码最长使用期限，0 表示永不过期；
密码最短使用期限，0 表示随时更改密码；
强制密码历史，0 表示无限制，可随意使用过去使用过的密码。

09. 普通用户登录密码错误次数达到了帐户锁定阈值后如何解锁？

锁定后可由管理员手动解除锁定；
锁定后可等锁定时间超时自动解锁。

10. 本地策略中用户权限分配的常用策略？

更改系统时间、关闭系统、允许本地登录、拒绝本地登录、拒绝从网络访问这台计算机。

11. 打开本地组策略及强制刷新策略的命令？

gpedit.msc　　//打开本地组策略
gpupdate　　/force 强制刷新组策略

12. 什么是 DNS，主要作用是什么？

DNS 即 Domain Name System，域名系统，端口号 53 。
主要作用： DNS 服务器可以为客户机提供“域名与 IP 地址”的地址解析服务

13. 常见顶级域名及含义？

1）组织域　　含义
- .gov　　政府
- .com　　商业
- .edu　　教育
- .org　　民间团体组织
- .net　　网络服务机构
- .mil　　军事部门

2)国家/地区域
- .cn　　中国
- .us　　美国
- .ru　　俄罗斯
- .hk　　中国香港
- .tw　　中国台湾

14. 简述常见的 DNS 资源记录类型，并描述各自的含义。

A
正向解析
PTR
反向解析（把 IP 地址映射为域名）
CNAME 别名解析

15. 活动目录的简称及特点？

活动目录简称 AD。
活动目录特点：集中管理，便捷的网络资源访问，可扩展。

16. 升级域控的条件有哪些？

1）安装者需具有本地管理员权限
2）有足够的可用磁盘空间
3）操作系统必须满足条件：Windows Server 版
4）静态 TCP/IP 设置（IP 地址，子网掩码）
5）需要有 DNS 服务器的支持
6）本地磁盘至少有一个分区是 NTFS 文件系统

17. GPO 是域中组策略设置对象，默认有哪两个 GPO？

默认域策略(Default Domain Policy)
默认域控制器策略(Default Domain Controllers Policy)

18. Windows 系统 SAM 文件的存储路径？

C:\Windows\System32\config\SAM

19. WinPE 系统中，磁盘管理工具的主要功能？

磁盘分区合并、磁盘分区释放、创建磁盘分区、磁盘格式化。

##

03.《网络通信原理- 作者：李宇龙》

##

01. OSI 模型每层的名称是什么？

从上往下依次为：

- 应用层
- 表示层
- 会话层
- 传输层
- 网络层
- 数据链路层
- 物理层

02. 什么是 PDU

PDU：协议数据单元

03. 数据在 TCP/IP 模型中每层的 PDU 分别叫什么名称？

应用层：数据
传输层：数据段
网络层：数据包
数据链路层：数据帧
物理层：比特流

04. MAC 地址是什么？

MAC 地址也叫物理地址，由 48 位二进制组成，前 24 位 表示的是厂商标识，后 24 表示的厂商自

己分配的编号。在前 24 位中：第八位为 0 表示的是单播 MAC 地址 ，第八位为 1 表示的是组播

MAC 地址。

05. 以太网数据帧的封装结构是什么？

目的地址 源地址 类型 数据 帧校验序列

06. ARP 协议的作用是什么？

ARP：地址解析协议

作用：是基于已知的目标 IP 地址，获得目标设备对应的 MAC 地址。

07. ARP 的分类有那些？

主要包括：

- 普通 ARP（正向 ARP）：通过 IP 地址获取 MAC 地址。
- 反向 ARP（RARP）：通过 MAC 获取 IP 地址。
- 免费 ARP：查询想使用的 IP 地址是否在局域网中已被占用。
- 逆向 ARP（IARP）：通过物理地址获取 IP 地址（一般出现在帧中继网络，实现 IP 和 DLCI 地址映射）。
- 代理 ARP：路由器收到 ARP request时，发现源IP和目标IP不在一个网段，就会当代理 ARP 角色，作为回答，告诉查询者它想要的 MAC 地址。

08. ARP 请求报文中的目的 MAC 地址是多少？

发送 ARP 请求报文时，目的 MAC 字段为全 0 的 MAC 地址 0x0000-0000-0000

09. 如何查看本机的 ARP 缓存表？如何清理本机 ARP 缓存？

查看 ARP 缓存：Win+R 打开运行，打开 cmd 命令行，输入 arp -a

清理 ARP 缓存：Win+R 打开运行，打开 cmd 命令行，输入 arp -d

10. 什么是静态 ARP？如何在本机配置静态 ARP 绑定？

静态 ARP：手工建立的 IP 地址和 MAC 地址之间固定的映射关系。

```
arp -s 主机地址 mac 地址
arp -s 192.168.222.4 00-50-56-ff-17-99
```

11. ICMP 是什么？ICMP 的作用是什么？

ICMP：Internet 控制消息协议、协议号 1、位于 TCP/IP 的第三层

作用：检测网络通信故障和实现链路追踪

12. ICMP 协议中两大应用？

ping 命令：检查网络是否畅通的常用命令

tracert 命令：用于确定 IP 数据包访问目标所采取的路径

13. ICMP 的常见回显消息代表什么意思？

```
Reply from 目标地址... 连接成功
Destination host unreachable 目标主机不可达
```

Request timed out 请求时间超时
Unknown host ... 未知主机名

14. IPv4 地址？

IP 地址：互联网协议地址
作用：标识一个节点的网络位置
长度：32 个二进制位
组成：网络位+主机位
表示方式：点分十进制
数量：2 的 32 次方

15. 什么是子网掩码？

子网掩码是长度和 IP 地址一样，由 32 个二进制位组成
作用：用来区分 IPv4 地址的主机位和网络位。
用 1 来表示网络部分
用 0 来表示主机部分 ‘’

16. 默认的子网掩码

A 类地址：255.0.0.0
B 类地址：255.255.0.0
C 类地址：255.255.255.0

17. 私有 IP 地址的分类及范围

A 类私有地址：10.0.0.0-10.255.255.255
B 类私有地址：172.16.0.0-172.31.255.255
C 类私有地址：192.168.0.0-192.168.255.255

18. TCP 是什么协议？TCP 协议的特点是什么？

传输控制协议：是一种面向连接的、可靠的的传输层通信协议。

19. UDP 是什么协议？UDP 协议的特点是什么？

用户数据报协议：非连接的协议、不可靠的的传输层协议。

20. Telnet 是什么协议？默认端口号是什么？

远程终端协议
端口号是 TCP 23

21. 什么是 AAA

AAA 是网络安全中进行访问控制的一种安全管理机制，提供认证、授权和计费三种安全服务。

22. TCP 三次握手的过程是什么？

第一次握手：建立连接时，客户端发送 syn 包（seq=j）到服务器。

第二次握手：服务器收到 syn 包，必须确认客户端的 SYN（ack=j+1），同时自己也发送一个 SYN

包（seq=k）即 SYN+ACK 包

第三次握手：客户端收到服务器的 SYN+ACK 包，向服务器发送确认包 ACK(ack=k+1)，此包发送

完毕，客户端和服务器 TCP 连接成功。

23. 什么是 DNS？

域名系统：用来完成域名与 IP 地址之间的映射，便于用户对网站的记忆和访问。

端口号是 TCP 或 UDP 的 53。

24. TFTP 是什么

简单文件传输协议

25. FTP 和 TFTP 的区别？

标准 FTP 端口号 TCP 21 和 22，标准 TFTP 端口号是 UDP 69。

FTP 用于稳定的传输大容量文件，TFTP 用来传输一些小的文件，速度快但是很容易丢包。

##

04.《弹性交换网络 - 作者：李宇龙》

##

01. 冲突域和广播域的区别是什么？

冲突域：就是连接在同一导线上的所有工作站的集合

交换机的每一个接口都是一个冲突域

02. 广播域：网络中能接收任一设备发出的广播帧的所有设备的集合

路由器的每一个接口都是一个广播域

03. 什么是 VLAN？VLAN 的作用什么？

VLAN：指的是虚拟局域网

VLAN 的作用：分割广播域

04. 部署 VLAN 的优势

限制广播域，节省带宽资源

增强局域网安全性

提高网络的健壮性

灵活的构建局域网

05. VLAN 的划分方式

基于接口的划分-主要应用方式
基于 MAC 地址的划分
基于子网的划分
基于协议的划分

06. VLAN 端口的主要类型（华为）

Access 接口：一般用于连接终端
Trunk 接口：一般用于连接交换机、路由器
Hybrid：即可以连接终端，也可以连接网络设备

07. Access 和 Trunk 的主要区别是什么

Trunk 链路一般用于交换机连接交换机，同一时刻可支持多个 VLAN 的数据转发，数据携带 VLAN
标签（native vlan 除外）。
Access 链路一般用于交换机连接终端，同一时刻只能传输一个 VLAN 的数据，发送数据的时候
剥离 VLAN 标签。

08. 交换机的工作流程是什么？

学习=>广播=>转发=>更新。

09. 如何恢复接口上 VLAN 的缺省配置？

对于 access 口：
先把端口恢复到默认的 vlan1，例如的 port default vlan 1，再去修改接口类型。
对于 trunk 口：
先恢复默认允许的 vlan1，如果是允许了所有 vlan，需要删除 undo port trunk allow-pass
vlan 2 to 4094。

10. 路由器的工作原理是什么？

路由器根据路由表转发数据包，当路由器收到一个数据包后，会查找路由表中是否存在这个数据包的目的地址。如果存在，就按此条路由条目的下一跳地址进行转发，如果不存在，则丢弃此数据包。

11. 什么 STP 协议？什么是 RSTP，什么是 MSTP？

STP：是生成树协议。
RSTP：快速生成树协议
MSTP：多生成树协议

12. STP 的作用？

当 2 层网络存在冗余链路的情况下，用来防止 2 层数据转发环路的发生。

13. STP 中桥的优先级默认是多少？步长值是多少？

默认优先级是 32768，步长是 4096。

14. STP 中，端口优先级默认是多少？

默认是 128。

15. 简述 STP 的工作原理？

默认情况下，交换机启动了 STP 功能。加电开机后，通过与相连的交换机互相发送和比较 BPDU ，从而确保网路中去往任何设备，仅存在一条最短的、无环、2 层数据转发路径。

具体过程如下：

1）首先确定交换机的角色：根交换机和非根交换机；

2）其次确定端口的角色：根端口、指定端口和非指定端口；

3）最后确定端口的状态：down、listening 、learning、forwarding、blocking

16. STP 根交换机的选举原则是什么？

通过比较每个交换机的 BID （桥 ID）来确定。

首先比较其中的优先级，值越小越好，默认值是 32768，步长是 4096，最优是 0；

如果优先级相同，则比较其中的 MAC 地址，值越小越好。

17. STP 如果选举根端口？

在非根交换机上，有且只有一个，看接口到根交换机的路径成本。

规则 1：非根交换机上到根交换机花费最小的端口就是根端口

规则 2：当到根交换机 Cost 值相同的时候，比较发送者的 BID

规则 3：当 Cost 的值和发送者的 BID 的值都相同时，比较发送者的 PID

规则 4：当发送者的 PID 也相同的情况下，比较接收者的 PID

18. 如何选举指定端口？

作用：专门用来发送 BPDU 报文（发送根桥指令的）

规则 1：比较到根交换机最小的 cost 值

规则 2：cost 值相同时，两台交换机相互比较 BID，PID

定律 1：根网桥上的所有端口都是指定端口

定律 2：一个网线上的一个端口是根端口，那另外一个端口肯定是指定端口

定律 3：每个端口只能承担一个角色

定律 4：同一条链路上，有且仅有一个指定端口

19. MSTP 和 RSTP 对比，有什么优势？

多生成树协议：继承了 RSTP 优点，引入了实例（instance）的概念，实现基于实例的负载均衡。

不但可以实现多个链路之间的备份，还可以提高多个链路的利用率。

20. 生成树协议中，交换机的 BPDU 类型有哪些？

配置 BPDU 和拓扑变更 BPDU。

21. RSTP 中的交换机端口的角色和状态有哪些？

端口角色：

根端口、指定端口、替代端口（替代的是根端口）、备份端口（备份的是指定端口）。

端口状态：

- Learning，学习状态；
- Forwarding，转发状态；
- Discarding，丢弃状态。

22. 链路聚合 Eth-Trunk 的作用？

Eth-Trunk（链路聚合）作为一种捆绑技术，可以把多个独立的物理接口绑定在一起，作为一个
大宽带的逻辑接口使用。优点：可以增加设备之间的互联带宽、提高设备之间的可靠性、对流量负载均衡，提高链路利用率。

23. 手工链路聚合的特点？

当两台设备中至少有一台不支持 LACP 协议时，可以使用手工负载分担模式的 Eth-Trunk。

手工负载分担模式下，加入 Eth-Trunk 的链路都进行数据转发。

24. LACP 链路聚合的特点

LACP 模式也称为 M:N 模式，其中 M 条链路处于活动转发状态，N 条链路处于非活动状态作为备份
状态。

25. 系统 LACP 的默认优先级是多少

默认优先级 32768，提供了一种通过 vlan 进行网络资源控制的机制，通过 MUX VLAN 提供的二层

流量隔离的机制。可以实现企业内部员工之间互相通信。而企业外来访客之间是互相隔离的。

26. 手工链路聚合和 LACP 链路聚合的区别？

手工模式：不需要支持 LACP 协议、正常情况下，所有链路都是活动链路 、无法检测链路错连

LACP 模式：需要支持 LACP 协议、正常情况下部分链路是活动链路、可以检测链路错连

27. 堆叠和集群的区别？

区别在于盒式交换机只能用堆叠,框式交换机只能用集群

28. 集群建立过程中主备交换机选举原则？

- 最先完成启动，并进入单框集群运行状态的交换机成为主交换机。
- 当两台交换机同时启动时，集群优先级高的交换机成为主交换机。
- 当两台交换机同时启动，且集群优先级又相同时，MAC 地址小的交换机成为主交换机。

■ 当两台交换机同时启动，且集群优先级和 MAC 地址都相同时，集群 ID 小的交换机成为主
交换机。

29. 什么是直连路由？什么是静态路由？静态路由如何配置？

路由的自身接口配置 IP 地址、保持接口 UP 状态，会在路由表里形成直连路由
由管理员手动添加，单向条目，一般在小型网络使用，不耗费设备资源、不灵活。
格式：

```
ip route-static 目标网络 掩码 下一跳
```

30. 路由表的作用？

由多条路由条目组成的，每一条路由条目都由数据访问的目标网段，以及从本设备哪个接口发出，
数据发送的下一个设备是谁等组成 ，指三层数据包进行数据转发。
格式：

```
display ip routing-table
```

31. 路由协议优先级的作用

区分不同的路由来源，表示的是路由的稳定性（数值越小越优），静态路由优先级是 60，直连路
由的默认优先级是 0。

32. 静态路由如何修改路由优先级？

比如设置某静态路由的优先级为 50：

```
ip route-static 172.16.1.1 32 192.168.0.1 preference 50
```

33. MUX VLAN 的类型？

主 VLAN、辅助 VLAN（组 VLAN 和隔离 VLAN）。

34. 在 Mux-VLAN 中隔离 VLAN 和组 VLAN 有什么不同？

同一个隔离 vlan 间的端口之间，不能互通。
同一个组的 vlan 端口可以互通，不同的组 vlan 之间的端口，不可以互通

35. VLAN 聚合的类型？

分为：Super-VLAN（超级 VLAN）、Sub-VLAN（子 VLAN）

36. VLAN 聚合的作用？

在多个 VLAN 的环境中节省 IP 地址

37. VLAN 聚合的优势？

Sub-VLAN 公用一个网关，节省 IP 地址
实现了不同广播域使用同网段地址，增加了编制的灵活性，避免了 IP 地址的浪费。

38. DHCP 的作用是什么？

动态主机配置协议，可以给电脑，手机等连网设备分配 IP 地址、子网掩码、网关、DNS。

39. DHCP 的角色有哪些？

DHCP 服务器，DHCP 客户端，DHCP 中继

40. DHCP 首次接入的过程？

主要过程：
1）发现阶段 Discover
2）提供阶段 Offer
3）选择阶段 Request
4）确认阶段 ACK

41. 在 DHCP 中设置排除地址的作用是什么？

把排除的地址保存下来，不参与地址的分配

42. DHCP 中继一般配置在那个设备上？DHCP 中继如何配置？

只有 DHCP 客户端的网关接口，才有资格成为 DHCP 中继。
配置过程：
1）开启 DHCP 中继 DHCP 功能
2）设置 DHCP 中继接口的模式为 relay
3）指定 DHCP 中继接口的 DHCP 服务器地址

43. 配置完 DHCP 后，无法获取到 IP 地址，应该怎么排错？

排错防范：
1）查看地址池是否配置正确。
2）DHCP 路由器上指向客户端网段的路由是否配置。
3）查看是否在相应的接口下配置了 dhcp select [global/interface/relay] 。
4）如果配置 DHCP 中继，检查 dhcp 中继有没有配置，是否配置正确。中继服务器的 IP 地址是否
正确。

44. 针对 DHCP 的常见攻击行为有哪些？

仿冒 DHCP Server 攻击，DHCP 饿死攻击

45. DHCP Server 仿冒攻击原理是什么？

客户端以广播方式发送 Discover 消息后，仿冒 DHCP Server 和合法的 DHCP Server 都能够收到

该 Discover 消息，并且都会回应 Offer 消息，如果客户端最先收到的 DHCP Offer 消息是来自

仿冒 DHCP Server，那么客户端就会继续向仿冒 DHCP Server 请求获得 IP 地址等参数，而仿冒

DHCP Server 就会向客户端分配错误的 IP 地址及网关地址等参数。

达内网络安全学院

##
05.《园区网实现与安全- 作者：李宇龙》
##

01. VRRP 是什么？
虚拟路由器冗余协议

02. VRRP 可以解决什么问题？
网关的单点故障问题

03. VRRP 的组播地址？协议号是多少？
组播地址 224.0.0.18，协议号是 112。

04. VRRP 角色有哪些?
Master 路由器、 backup 路由器、虚拟路由器。

05. VRRP 主备角色选择原则是什么?
对比优先级，越大越好。
对比 IP 地址，越大越好。

06. VRRP 如何实现负载分担？
原有 VRRP 的方法，路由器得不到有效利用。
不通的网段的流量分别走不通的路由器， 而另一个路由器作为备份。这样既实现了备份， 也实现 了负载均衡。

07. VRRP 工作过程简述?
主要包括：
1）主网关周期性发送 VRRP 通告报文（三层心跳报文）。
2）通告报文发送的周期时间：默认情况下是 1 秒。
3）通告报文发送的目的地址是组播地址： 224.0.0.18。
4）备份网关监控主网关状态， 在 3 倍的"发送周期"后， 如果无法收到主网关发送的 VRRP 通告 报文，备份网 关升级为“主网关”，承担流量转发任务。

08. BFD 的作用是什么？
BFD：双项转发检查机制，用于快速检测、监控网络中链路或者 IP 路由的转发连通状况。

09. BFD 的原理是什么？
BFD 的检测机制是两个系统建立 BFD 会话， 并沿它们之间的路径周期性发送 BFD 控制报文，如果一方在既定的时间内没有收到 BFD 控制报文， 则认为路径上发生了故障。

10. 什么是网关？

即一个网段去往另外一个网段时的出口。

11. 子网划分的原因是什么？

满足不同网络对 IP 地址的需求，实现网络的层次性，节省 IP 地址。

12. ACL 的作用是什么？

ACL，指的是访问控制列表，作用是匹配感兴趣流量。
很多不同的控制工具，都可以调用 ACL，然后实现不同的控制结果。

13. ACL 的类型有哪些，分别在什么情况下使用？

基本 ACL：
只能匹配数据包的源 IP 地址；通常情况下应用在控制数据包不精确的工作场景下。 高级 ACL（扩展 ACL）：
可以匹配数据包的源 IP、目标 IP、协议号、源端口和目标端口等信息。通常情况下应用在控制数据包“精准”的工作场景下。

14. ACL 的隐藏规则及特点？

隐藏规则：
华为 acl 有一条默认的隐含规则，是允许所有。在 acl 和 traffic-filter 联动的时候，如果一个数据包没有匹配到 acl 中的任何一条规则，则执行 acl 中的隐含规则，允许所有。
如果使用 acl 隐含规则，需要满足两个条件，一个是在 acl 和 traffic-filter 联动的时候，一个是数据包不能匹配到 acl 中的任何一条规则，只有满足这两个条件，才会应用隐含规则。
华为 acl 还有一个隐含规则， 是拒绝所有， 当 acl 没有和 traffic-filter 联动的时候，acl 的默认都是拒绝所有。
主要特点：
acl 对设备本身（自己）发起的流量是不起作用，只对经过的流量起作用。
acl 与 traffic-filter 结合使用时，且不能匹配到任何规则，最后有一个隐含规则“允许 所有”。
acl 没有和 traffic-filter 联动的时候， 且不能匹配到任何规则， acl 的默认隐含的条目是 拒绝所有。

15. NAT 是什么及分类？

网络地址转换，内网私有地址转换公网公有地址，通常配置在企业边界网关上面，保护内网主机， 提高安全性。
分类分为（1）静态NAT---1对1 ，不节省IP地址。
动态 NAT--- 多对多 ，但是本质还是1对1 ，公有地址有多少同时上网的主机数就有多少。

16. 基本 NAT 和 NAPT 的区别是什么？

两者的区别在于NAPT不仅可以转换数据包中的IP地址，还可以对IP包中TCP和UDP的端口进 行转换，普通的基本NAT都是只基IP地址进行转换。

17. Easy-ip 是什么？ 地址池 NAT 是什么？ 它们的区别是什么？

Easy-ip 是 NAPT 的一种特例属于单向转换，配置的时候不需要创建公网地址池。
地址池 NAT 通过设置公网地址池通过动态分配的方式，共享很少的几个公网 IP 地址，全部占用后，后续的 NAT 申请将会失败。
区别在于 Easy-ip 采用的是网络接口地址，所有内网 IP 使用接口地址访问外网，地址池 NAT 采 用的是独立地址池中的地址做转换而不使用接口地址。

##

06.《园区网路由- 作者：李宇龙》

##

01. OSPF 的工作原理？

主要过程：
1）建立邻居关系
2）同步数据库
3）计算路由表

02. OSPF 的报文有哪些？

主要报文：
- Hello 用来建立维护邻居关系
- DD 用来发送数据库摘要信息
- LSR 用来向对端请求本端数据库没有的信息
- LSU 回应对端请求的信息
- LSACK 回应对方的更新信息

03. OSPF 网络类型有哪些？

- 广播类型（Broadcast）
- 非广播类型（NBMA）
- 点到点类型（P2P）
- 点到多点类型（P2MP）

04. DR 的作用是什么？

- 减少邻接关系，降低设备负担
- 降低 OSPF 协议流量
- 加快数据库同步

05. DR 的选举原则是什么？

接口首先比较优先级，数值越大越优先

如果接口的优先级相等时，则比较 Router ID，数值越大越优先

06. Router-id 的作用是什么？

路由器标识 即路由器的名字,每个运行 OSPF 的路由器都会有一个名字，全网唯一。

07. OSPF 有哪些区域？

骨干区域： area0
非骨干区域：除 area 0 之外的其他所有许可范围内的区域
特殊区域： stub、totally stub、NSSA、totally NSSA

08. 特殊区域的作用？

保护一个区域不受来自外部链路的影响
缩减 LSDB 和路由表的规模，减少路由信息数量，降低设备压力

09. 什么是 ABR？什么是 ASBR？

ABR：区域边界路由器， 位于一个或多个 OSPF 区域边界上， 将这些区域连接到主干网络的路由器
ASBR：自治系统边界路由器，位于 OSPF 自治系统和非 OSPF 网络之间。

10. OSPF 路由聚合的作用？

可以减少路由信息，从而减小路由表的规模，提高交换机的性能

11. 配置 Stub 区域时需要注意下列几点？

- 骨干区域不能配置成 Stub 区域。
- 如果要将一个区域配置成 Stub 区域，则该区域中的所有交换机都要配置 STUB 区域属性。
- Stub 区域内不能存在 ASBR，即自治系统外部的路由不能在本区域内传播。

12. OSPF 的路由类型有哪些？

主要包括：

- 1 类 LSA=Router-id
- 2 类 LSA=Network
- 3 类 LSA=Summary
- 4 类 LSA=ASBR
- 5 类 LSA=External 外部路由
- 7 类 LSA=NSSA

13. OSPF 建立邻居的状态有哪些？

主要包括：

- Down 设备彼此之间谁不知道谁
- Init 收到对方的信息，但是对方不知道自己

- 2-way 彼此都知道对方是谁
- Exstart 确定谁是主动端，主动与对端交互信息
- Exchange 开始发送数据库简要信息 ，彼此进行对比交互
- Loading 通过数据库摘要信息，发现本端没有的信息发送 lsr 请求消息、对方通过 update 更新，本端通过 lsack 进行确认
- Full 达到同步数据库的完美状态

##

07.《骨干网规划与实现- 作者：李宇龙》

##

01.BGP 是什么？

BGP（Border Gateway Protocol）是一种用于自治系统 AS（Autonomous System）之间的动态路 由协议。

02.组建 BGP 网络最基本的配置过程？

1)创建 BGP 进程 （创建 AS 号） ：只有先创建 BGP 进程，才能开始配置 BGP 的所有特性。
2)建立 BGP 邻居关系：只有成功建立了 BGP 邻居关系，设备之间才能交换 BGP 消息
3)注入路由：BGP 协议本身不发现路由，只有引入其他协议的路由才能产生 BGP 路由。

03.BGP 消息类型？

Open:用于 BGP 邻居的建立，协商参数
Updata：用于 BGP 邻居之间传递路由条目
Keep-alive:用于 BGP 邻居之间的维护，周期发送时间 60s,180s 收不到认为邻居断开
Notification:通知报文，用于在 BGP 邻居之间传递报错信息
Route-refresh:请求邻居发送路由信息

04.BGP 路由注入的方式？

Import 方式是按协议类型，将 RIP 路由、 OSPF 路由、静态路由和直连路由等某一协议的路由注 入到 BGP 路由表中。
Network 方式比 Import 方式更精确，将指定前缀和掩码的一条路由注入到 BGP 路由表中

05.什么是水平分割原则？ BGP 为什么要有水平分割？

BGP 路由器通过 IBGP 邻居获得的最优路由不会发布给其他的 IBGP 邻居，IBGP 水平分割原则用 于防止 AS 内部产生环路。

06. 路由反射器的作用？

为保证 IBGP 对等体之间的连通性，需要在 IBGP 对等体之间建立全连接关系。当 IBGP 对等体数 目很多时，建立全连接网络的开销很大。使用路由反射器 RR，可以解决这个问题。

07. 联盟的作用？

联盟（Confederation）是处理 AS 内部的 IBGP 网络连接激增的一种方法， 它将一个 AS 划分为若 干个子自治系统（Sub AS），每个子 AS 内部建立 IBGP 全连接关系，子 AS 之间建立 EBGP连接关系

08. 路由反射器的反射规则？

从非客户机 IBGP 对等体学到的路由，发布给此 RR 的所有客户机。

从客户机学到的路由，发布给此 RR 的所有非客户机和客户机（发起此路由的客户机除外）。

从 EBGP 对等体学到的路由，发布给所有的非客户机和客户机。

从非客户机 IBGP 对等体学到的路由， 不会发布给非客户机。

09. 反射器和联盟的区别？

1)反射器不需要改变现有网络拓扑，兼容性好；联盟需要概念拓扑结构

2）反射器配置方便， 只需要对作为反射器的设备进行配置， 客户机并不需要知道自己是客户机； 联盟： 所有设备需要重新进行配置。

3)反射器适用于中、大规模网络；联盟适用于大规模网络；

10. MED 与本地优先级的区别？

本地优先级：

本地优先级属性，数值越大越好，默认是 100

该属性能在 AS 内部任意传递，不能在 AS 之间传输

用于判断流量离开 AS 时的最佳路由

MED:

开销值属性，默认为 0，越小越好

该属性可以在 AS 之间传递

用于判断流量进入 AS 时的最佳路由

11. BGP 路由的来源有哪些？

IGP：BGP 用 network 命令注入到路由表的路由， 优先级最高

EGP：通过 EGP 得到的路由信息， 优先级次之

Incomplete：表示路由的来源无法确定。 BGP 通过 import-route 命令引入的路由， 优先级最低

12. AS-PATH 属性的作用？

AS_Path 数量可以作为 BGP 选路条件，AS-Path 通过携带路径属性也可用于 AS 之间的防环

13. 给网络设备接口配置 IPv6 地址的步骤及命令？

系统视图先开启 ipv6 功能，然后进入接口视图开启 ipv6 之后配置地址即可。 命令参考：

```
[Huawei]ipv6
[Huawei]int g X/X/X
[Huawei-GigabitEthernetX/X/X]ipv6 enable
```

14. 查看 IPv6 路由表的命令？

```
[Huawei]display ipv6 routing-table
```

15. 查看 OSPFv3 邻居的命令？

```
[Huawei]display ospfv3 peer
```

16. OSPFv3 和 OSPFv2 的主要区别？

OSPFv3 主要支持基于 IPv6 的网络环境， OSPFv2 主要支持 IPv4，两者所服务的 IP 协议不同

OSPFv3 直接在接口加入区域的设置即可把接口的网段宣告，而 OSPFv2 需要到区域里面宣告网段， 两者宣告网段的方式也有所不同。

17. AP 是什么？ AP 的分类有哪些？

AP 即无线访问接入点，功能类似于家里的无线路由器， 可以覆盖几十米至上百米。 主要包括：胖 AP、瘦 AP。

胖 AP---家庭或者办公室使用，单独管理，需要接入电源。

瘦 AP---做统一 的无线覆盖用的，使用AC 控制统一 管理，不需要接入电源，由 POE 供电交换机，

通过网线提供电力。

18. 什么是 POE 供电交换机？

即具备 POE 供电模块的交换机，可以给无线 AP 提供电力能源。

19. WLAN 是什么？

WLAN 指的是无线局域网， 指应用无线通信技术将计算机设备互联起来， 构成可以互相通信和实现资源共享的网络体系。

20. 常见的无线网络架构？

AC 直连式组网

AC 旁挂式组网

21. 请描述 WLAN 网络中的数据转发方式？

隧道转发方式：隧道转发方式是指用户的数据报文到达 AP 后，需要经过 CAPWAP 数据隧道封装后发送给 AC，然后由 AC 再转发到上层网络

直接转发方式：直接转发方式是指用户的数据报文到达 AP 后，不经过 CAPWAP 的隧道封装而直接转发到上层网络

达内网络安全学院

##
09.《网络安全解决方案- 作者：胡新亮》
##

01. 什么是下一代防火墙？

下一代防火墙是一款可以全面应对应用层威胁的高性能防火墙。
通过深入洞察网络流量中的用户，应用和内容，能够为用户提供有效的应用层一体化安全防护。

01. 下一带防火墙的主要特性？（至少写出三个）

主要包括：

- 行为管控与带宽管理
- VPN 部署与智能路由
- 内容安全与数据防泄漏
- 入侵防御与 WEB 防护
- 应用识别与管控
- APT 防御与 Anti-DDOS
- 云管理与云安全感知

02. 写出你了解的防火墙厂商（至少写三个）

主要包括：

- 华为 USG 系列 AI 防火墙（NGFW）
- 深信服下一代防火墙（NGAF）
- 天融信下一代防火墙（NGFW）
- 启明星辰-天清汉马 T 系列防火墙
- 绿盟防火墙（NF）
- 奇安信新一代智慧防火墙
- 安恒-明御安全网关（NGFW）

03. 华为交换机默认的安全区有那几个（至少写出三个）

Untrust：安全级别5，用于定义互联网流量
DMZ：安全级别50，用于定义服务器区域
Trust：安全级别85，用于定义内网所在区域
Local：安全级别100，用于定义设备收发的流量

04. 如果公司内部的主机需要上网，请写出你了解的地址转换方案

Easy IP ：基于出接口的NAPT，用于只有一个公网IP、公网IP不固定、内网主机少的场景。
地址池NAT：基于地址池的NAPT，如果有多个公网IP地址

05. VPN 是什么？

VPN全称Virtual Private Network，中文含义虚拟专用网，可以在不改变现有网络架构的情况下，两地局域网通过Internet建立虚拟专用连接，以进行安全、可靠的数据传输。一般用于**分公司**和**总部**之间网络互联，或用于**员工**接入到**公司内部**网络

06. VPN 的特点？

使用加密技术防止数据被窃听。
数据完整性验证防止数据被破坏，篡改。
通过认证机制确认身份，防止冒充。

07. VPN 的优势？

安全：专用连接。
廉价：利用公共网络，建立虚拟隧道进行数据通信。
支持移动业务：任何时间，任何地点都可以使用VPN。
可扩展性强：VPN为逻辑网络，物理网络改变，不影响VPN部署。

08. 常见的 VPN 类别？

主要包括：

IPSec VPN：用于站点到站点
L2TP VPN：用于员工远程访问
SSL VPN：用于员工远程访问
BGP/MPLS VPN：用于运营商专线网络

09. IPSEC VPN 的配置步骤有哪些？

主要包括：

1）配置接口地址
2）配置对象
3）配置安全策略
4）配置路由
5）配置IPSEC VPN
6）定义名称
7）定义对端地址
8）定义预共享秘钥
9）定义待加密的数据流
10）定义安全提议

10. 什么是策略路由？

策略路由是在路由表已经产生的情况下，不按照现有路由表进行转发，而是根据用户制定的策略进行路由选择的机制，从更多的维度（入接口、源安全区域、源/目的IP地址、用户、服务、应用）来决定报文如何转发，增加了在报文转发控制上的灵活度。策略路由并没有替代路由表机制，而是优先于路由表生效，为某些特殊业务指定转发方向

11. 策略路由的组成？

策略路由组成：匹配条件、动作
匹配条件包括：入接口/源安全区域，IP地址/MAC地址（源、目的），用户、服务、应用、时间段，DSCP优先级：进行流量类型识别
实施策略路由动作包括：转发单出口（下一跳）、多出口（智能选路），不做策略路由：按照现有路由表进行转发

12. 策略路由的匹配过程？

先寻找第一条规则，如果满足条件执行动作；
如果不满足第一条规则的匹配条件，寻找下一条规则；
如果所有的策略的匹配条件都无法满足，则按照路由表转发。

13. 双机热备的部署方式有那些？

主要包括：

- 热备
- 负载分担

##

10.《Windows渗透测试- 作者：胡新亮》

##

01. 木马、病毒的特点分别是什么？

木马以控制目标主机或窃取数据为主要目标，一般不易察觉；病毒以破坏主机系统或数据为主要目标，产生的影响如占用资源使主机卡顿、使主机崩溃、数据被破坏等。

02. 漏洞利用的危害有哪些？

黑客可以利用系统或程序漏洞，对目标主机进行安装非法程序、执行非法指令、获取管理权限等。

03. 系统扫描能获得哪些信息？

通过系统扫描操作，可以获得目标主机的系统类型、软件版本、开放的端口、存在的漏洞等信息。

04. 什么是网络钓鱼？

黑客可以通过制作高度相似的假冒网站，诱骗用户访问以骗取账号、密码等信息。

05. 什么是 DoS 攻击、DDoS 攻击？

DoS，拒绝服务攻击，指的是通过大量访问耗尽目标主机资源，从而导致正常用户无法访问受害站点的攻击手段。DDoS，分布式拒绝服务攻击，指的是组织成千上万甚至更多的攻击机（肉鸡），在同一时间向同一个目标发起DoS攻击，这种攻击方式成本更大，攻击的效果也更大，防护难度也很大。

06. 简述“网络安全法”和“等级保护”的关系。

《网络安全法》是《网络安全等级保护》实施的法律依据，能够推动网络安全等级保护制度的贯彻落实。而“等级保护”可以引导互联网运营者更强执行《网络安全法》规定的网络安全维护义务，让我们更易于了解网络安全维护义务必须做些哪些，自身现阶段做得怎样，有哪些地方不够，必须怎么改善等。

07. 简述网络安全等级保护工作实施的基本流程。

网络安全等级保护工作实施基本流程有5个阶段：保护对象定级与备案、总体安全规划、安全设计与实施、安全运行与维护、定级对象终止。

08. 描述等级保护分级的 5 个级别。

网络信息系统安全等级保护分为五级，防护水平一级最低，五级最高。具体介绍如下：

第一级、自主保护级，一般适用于小型私营、个体企业、中小学，乡镇所属信息系统、县级单位中一般的信息系统。不需要备案，对评估周期没有要求。

这类信息系统遭到破坏后，将对公民、法人和其他组织的合法权益造成普遍损害，但不会影响国家安全、社会秩序和公共利益。

第二级、指导保护级，一般适用于县级其他单位中的重要信息系统;地市级以上国家机关、企事业单位内部一般的信息系统，比如非涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统等。

公关机关备案，建议两年评估一次。此种信息系统被破坏后，将严重损害公民、法人和其他组织的合法权益。会对社会秩序、公共利益造成一般损害，不损害国家安全。

第三级、监督保护级，一般适用于地市级以上国家机关、企业、事业单位内部重要的信息系统，比如涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统。

公安机关备案，要求每年检测一次。这类信息系统被破坏后，将对国家安全和社会秩序造成危害，对公共利益造成严重损害，尤其是对公民、法人和其他组织的合法权益造成严重损害。

第四级：强制保护级，一般适用于国家重要领域、重要部门中的特别重要系统以及核心系统。例如电力、电信、广电、铁路、民航、银行、税务等重要、部门的生产、调度、指挥等涉及国家安全、国计民生的核心系统。

公安部门备案，要求半年一次。此类信息系统受到破坏后，会对国家安全造成严重损害，对社会秩序、公共利益造成特别严重损害。

第五级：专控保护级，一般适用于国家重要领域、重要部门中的极端重要系统。

公安部门根据特殊安全需要备案。这类信息系统被破坏后，将特别严重地损害国家安全。

09. 简述等级保护体系基本框架。

等级保护2.0体系架构从技术和管理两个维度提出了具体的安全防护要求：

技术要求包括：安全物理环境、安全通讯网络、安全区域边界、安全计算环境、安全管理中心，其核心是“一个中心三重防御”。

管理要求包括：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。

10. kali 系统中，给普通用户提权的命令？

sudo -i

11. 什么工具可以用来探测目标网络或主机？

Nmap、ping、Nessus、OpenVAS、AppScan等

12. DOS 攻击是什么？

拒绝服务攻击：无论通过何种方式，最终导致目标系统崩溃、失去响应，从而无法正常提供服务或资源访问的情况。

DoS 攻击中比较常见的是洪水方式，如 SYN Flood、 Ping Flood。

13. DDOS 攻击是什么？

分布式拒绝服务攻击：典型的流量攻击，攻击方的主机数量呈现规模化

通常由分布在不同网络，不同位置的成千上万的主机组成，称为botnet僵尸网络，被同一发起攻击者控制

DDOS攻击强度更大，防御难度也更大

14. Crunch 字典工具的常用选项有那些？

crunch <密码长度最小值> <密码长度最大值> <生成密码的字符>

-d：字符可以连续的个数。比如2，密码最多2位连续。

-o：输出密码字典。

-t：已知密码某些的位。如123%%%，已知密码前三位为123。

15. 公司网站经常受到 DDOS 攻击，如何防御？

常见防御措施：

- 减少服务配置的等待时间
- 优化单一客户机的并发响应策略
- 更换高性能设备
- 增加网络带宽
- 采用负载均衡架构
- 部署 CDN 内容分发网络
- 冰盾防火墙
- 流量清洗、 DDoS 高防 IP
- IDS 入侵防御设备
- 抗 DDoS 专用防火墙设备

16. 使用 hydra 工具时，调用密码字典发起暴力破解的基本用法？

hydra -l 用户名 -P 密码字典文件 -s 目标端口 目标地址 服务类型

17. 渗透测试是什么？

是一种通过模拟攻击的技术与方法，打破目标系统的安全防御，并获得目标系统控制访问权的安全测试方法。

渗透测试目标分类有那些？

- 针对主机操作系统渗透：Windows、Linux、……

- 针对数据库系统渗透：MySQL、MS-SQL・・・
- 针对应用系统渗透：PHP 组成的网站・・・
- 针对网络设备渗透：防火墙、路由器、交换机・・・

18. 渗透测试的 7 个阶段？

1）前期交互
2）信息收集
3）威胁建模
4）漏洞分析
5）渗透攻击
6）后渗透攻击
7）渗透报告

19. 常见的漏洞披露平台有那些？

1）微软安全公告/微软应急响应中心。https://msrc.microsoft.com
2）CVE：通用漏洞与披露。http://cve.org
3）CWE：通用缺陷列表，也叫常见弱点列表。http://cwe.mitre.org
4）国家信息漏洞共享平台。https://www.cnvd.org.cn
5）美国国家信息安全漏洞库。https://nvd.nist.gov
6）腾讯安全应急响应中心。https://security.tencent.com
7）阿里安全应急响应中心。https://security.alibaba.com/

20. OpenVAS 执行基本扫描的步骤是什么？

1）配置扫描端口
2）添加扫描目标
3）指定扫描配置
4）创建扫描任务
5）生成扫描报告

21. MSF 漏洞框架是什么？

MSF是Metasploit Framework漏洞框架的简称，是一款开源的安全漏洞检测工具。可以收集信息、探测系统漏洞、执行漏洞利用测试等，为渗透测试、攻击编码和漏洞研究提供了一个可靠平台。

22. Msfconsole 控制台的常用操作命令？

exit //退出MSF控制台
show //查看模块或相关信息
search //搜索模块
use //使用模块
options //列出当前模块的选项
set //设置模块选项
run //运行当前模块

23. MSF 的主要模块有哪些？

Auxiliary：主要执行扫描、嗅探、指纹识别、爆破等相关功能以辅助渗透测试。
Exploits：应用或者服务中的安全漏洞进行的攻击行为。
Payloads：目标系统在被渗透攻击之后，在目标系统上运行任意命令或者执行特定代码。
Post：后渗透攻击动作，如获取敏感信息、实施跳板攻击等。
Evasion：该模块在渗透测试中负责免杀，以防止被杀毒软件、防火墙、IDS及类似的安全软件检测出来。
Encoders：编码器模块，主要包含各种编码工具，对payload进行编码加密，以便绕过入侵检测和过滤系统。
NOPS：不做任何操作，占位。

24. Windows 有哪些高危漏洞？

MS12-020 RDP 远程命令执行漏洞
MS15-034 IIS 远程命令执行漏洞
MS16-114 SMB 远程命令执行漏洞
MS17-010 SMB 远程命令执行漏洞
CVE-2017-5753 读取内存信息、数据泄露
CVE-2019-0708 RDP 远程命令执行漏洞

25. 成功渗透到 Windows 系统后，在 meterpreter 下如何获取主机用户名和密码？

```
# hashdump
```

26. 清除 Windows 安全事件日志的命令？

```
clearev -h
```

27. 成功渗透到 Windows 系统后，在 meterpreter 下，如何开启远程桌面功能？

```
# meterpreter > run post/windows/manage/enable_rdp
# meterpreter > run getgui -e
```

28. 成功渗透到 windows 系统后，在 meterpreter 下， 开启键盘记录的命令有那些？

```
# meterpreter > keyscan_start   //开启键盘记录功能
# meterpreter > run post/windows/capture/keylog_recorder
cat /root/.msf4/loot/2021122•••••••••••
```

29. Windows 中，UAC 是什么，作用是什么？

UAC，即User Account Control用户账户控制，是Windows操作系统中的一种安全控制机制。使用UAC，可以防止未经授权应用程序的自动安装，阻止恶意程序，防止系统损坏。

30. 瑞士军刀的作用？

Netcat（nc）被誉为网络安全界的“瑞士军刀”。

通过使用TCP或UDP协议的网络连接去读写数据，能够直接由其它程序和脚本轻松驱动。可以作为后门程序潜伏在受害者系统，开放指定端口随时连接。

31. 什么是 POC 脚本？

Proof of Concept“观点证明”，一段验证漏洞的程序，使我们能够确认这个漏洞是真实存在的。

##

11. 《Linux渗透测试- 作者：高昌勇》

##

01. 如何实现对 Linux 云服务器的远程管理， 用什么工具、什么协议、什么端口？

通过 SSH 方式远程管理 Linux 服务器。

常用的 SSH 客户端软件有 MobaXterm、Xshell、Putty 等。

使用 SSH 协议， TCP 22 端口号。

02. 你了解的常见的 Linux 系统有哪些？

Red Hat、CentOS，openEuler、Fedora、UOS 统信、 Deepin 深度、 UbuntuKylin 优麒麟、 Debian、Ubuntu 乌班图、 Kali 等。

03. 简述绝对路径、相对路径的含义？

绝对路径：以 / 开始的完整路径（或者以 ~ 开始的路径），与当前所在的目录位置无关。

相对路径：以当前工作目录为参照的路径。

04. 列出不少于 5 个常见的 Linux 目录，并描述各自的用途？

主要包括：

- /：整个 Linux 文件系统的根目录
- /boot：存放系统内核、启动菜单配置等文件
- /home：存放普通用户的默认家目录（同名子目录）
- /root：管理员的家目录 /bin、/sbin：存放系统命令、可执行的程序
- /dev：存放各种设备文件
- /etc：存放各种系统配置、系统服务配置文件

05. 你熟悉哪些厂商的云主机？

阿里云、华为云、百度云、腾讯云、亚马逊 AWS、微软 Azure。

06. 购买云主机你会关注哪些点？

主要包括：

计费模式、区域、CPU、内存、硬盘、带宽、监控、备份、安全合规

07. Linux 用户和组管理命令有那些？

```
# useradd   用户名
# passwd    用户名
# userdel  -r  用户名
# groupadd  组名
# gpasswd -a 用户名      组名
# gpasswd -d 用户名      组名
# groupdel   组名
```

08. Linux 系统中如何控制文档的访问权限？

设置文档归属：

```
#   chown  -R  属主:属组    文档 ...
#   chown  -R  属主    文档 ...
#   chown  -R  :属组    文档 ...
```

设置文档权限：

```
# chmod  -R  ugoa+-=rwx  文档
```

09. 简述文档归属、访问权限的类别及各自含义？

1）文档归属

属主：拥有此文件/目录的用户-user

属组：拥有此文件/目录的组-group

其他用户：除所有者、所属组以外的用户-other

2）访问权限

读取：允许查看内容-read

写入：允许修改内容-write

可执行：允许运行和切换-excute

10. 如何在 Linux 系统中找到你想要的文件？

使用 which 命令可以快速查找可执行文件，用法： which

使用 find 命令可以按条件查找文件，用法： find 目录 条件... 。

11. pgrep 与 pkill 命令各自的作用和区别？

pgrep 相当于 Process Grep，是用来根据关键词等条件快速找出进程的；

pkill 相当于 Process Kill，是用来根据关键词等条件快速杀死进程的。

12. sudo 操作的特点是什么，有什么好处？

主要特点：

1）日常维护操作通过普通用户登录，而不是以 root 直接登录

2）通过在命令行前添加 sudo 调用，普通用户也可以执行 root 授予的特权操作 3）需要 root 用户提前为特定用户授权特定的 sudo 调用权限

好处：
1）避免采用 root 密码直接登录带来的安全风险
2）将普通用户的权限最小化，提高安全性
3）管理员对普通用户通过 sudo 调用的命令可控、可通过日志跟踪

13. 禁止普通用户使用 su 切换操作，如何配置？

可以修改 /etc/pam.d/su 配置文件，启用 pam_wheel.so 限制。

```
# vim /etc/pam.d/su
auth            required        pam_wheel.so use_uid
```

然后把允许使用 su 的用户加入到 wheel 组，其他用户不要加入这个组就行了。

##

12.《网络安全防御- 作者：高昌勇》

##

01. 挂载/卸载光盘的命令是什么？

```
# mount /dev/cdrom   /xx/xx
# umount /xx/xx
```

02. YUM 是什么？作用是什么？

Yum: Yellow dog Updater, Modified 是一个 shell 前端软件包管理器。
作用：分发软件包资源、解决依赖关系、查询、安装、卸载软件。

03. YUM 两个配置文件路径分别是什么？

YUM 源配置目录（用来存放各种仓库设置文件）：/etc/yum.pepos.d/。
YUM 行为设置文件： /etc/yum.conf。

04. 快速配置 yum 软件源的命令是什么？

```
# yum-config-manager --add-repo  file:///软件源路径
```

05. Yum 管理命令有那些？

```
# yum list 软件名
# yum info 软件名
# yum provides 文件名
# yum -y install 软件名
# yum -y remove 软件名
# yum -y reinstall 软件名
```

06. 什么是 LAMP？包含那几个组件，作用分别是什么？

LAMP 是一种成熟的动态企业网站服务器模式，包含以下组件：

- Linux：作为服务器操作系统，提供运营平台

- Apache HTTP Server：作为最前端组件，负责处理 HTTP 访问请求
- MariaDB 或 MySQL：作为后端数据库，提供数据存储
- PHP 或 Python：作为后端开发环境，实现网页程序支持

07. 堡垒机的主要作用是什么？

- 主要包括：
- 访问控制：保障企业网络和数据的安全，不受来自内部或外部用户的入侵和破坏
- 资源授权：支持精细化访问权限，能够实时阻断违规、越权的访问行为
- 安全审计：能够对运维人员维护过程进行全面跟踪、控制、记录、回放，能够提供操作 全过程的记录和报告，满足国家等级保护 2.0 的要求

08. 常见堡垒机厂商？

主要包括：

- 启明星辰-天玥安全网关
- 安恒-明御运维审计与风险控制系统
- 天融信-运维安全审计系统
- 绿盟-运维安全管理系统 OSMS
- 飞致云-JumpServer 堡垒机--开源

09. jumpserver 堡垒机中， 资产指的是什么？

公司的服务器，被保护的服务器属于资产

10. jumpserver 堡垒机中， 用户有哪些类型？

堡垒机用户指的是公司员工用来登录堡垒机的账户，是在堡垒机上给员工分配的账户。

系统用户：普通用户是指，堡垒机登录被保护的服务器时使用的账户

特权用户：被保护的服务器本身自带的管理员账户

11. jumpserver 堡垒机中， 资产授权规则的作用是什么？

主要包括：

- 定义用户：员工登录堡垒机的用户
- 定义资产：是指员工可以访问那些服务器
- 定义系统用户：堡垒机用那个用户来远程被保护的服务器
- 定义访问权限：员工通过堡垒机远程服务器时，拥有那些权限

12. zabbix 体系架构中， zabbix-server、zabbix-agent 的作用是什么？

zabbix-server：作为 zabbix 服务端，负责采集、存储各种监控数据，并通过 Web 提供管理数据分析入口，以及监控结果展示界面。

zabbix-agent：作为 zabbix 客户端，安装在 Linux 或 Windows 服务器上，为 zabbix-server 提 供相应的监控数据。

13. 配置 zabbix 服务器的数据库连接时，需要修改或确认几个关键语句？

```
# vim /etc/zabbix/zabbix_server.conf
DBName=Zabbix          //数据库名
DBUser=Zabbix          //数据库用户
DBPassword=pwd@123     //连接密码
```

14. zabbix 服务器是如何获取路由交换设备或 Linux 主机信息的？

Zabbix 是一套集中展示网络设备、主机信息的开源监控平台， 通过C/S模式采集数据，通过B/S模式在 WEB 端展示和配置。

由zabbix server通过 SNMP，zabbix agent，ping，端口监视等方法获取被监控设备信息。

zabbix agent需要安装在被监控的目标服务器上，主要完成硬盘、内存、CPU等硬件信息的收集。而对于路由器、交换机等网络设备，则通过SNMP协议向 zabbix server提供监控信息。

15. 配置 zabbix-agent 被控端时，需要修改的关键参数有哪些？

需要配置 zabbix-agent 被控端，允许 zabbix 主控端采集监控数据。

```
# vim /etc/zabbix/zabbix_agentd.conf
Server=192.168.10.223           //添加 Zabbix 服务端的 IP 地址
ServerActive=192.168.10.223     //添加 Zabbix 服务端的 IP 地址
Hostname=svr8.tedu.cn           //本机的主机名
```

##
14.《WEB 应用基础 - 作者：刘闯》
##

01.什么是 WEB

全称是 World Wide WEB，中文名称是“全球广域网”或“万维网”
表现形式是超文本、超媒体、超文本传输协议。

02.Web 应用服务器由哪几部分组成？

Web 服务器，如 Apache、IIS、Tomcat 等
Web 应用程序，如 PHP、Python、JAVA 等
Web 数据库服务器,如 MySQL、Oracle、SQL Server 等

03.什么是 HTML？HTML 的作用和特点是什么？

HTML 是 HyperText Markup Language 的缩写，超文本标记语言
HTML 用来设计网页，包括如下特点：

- 通过标签的形式构建页面结构和填充内容
- 由浏览器解释执行
- 文件以.html 或.htm 为后缀,也称 web 页面
- HTML 不是一种编程语言,而是一种标记语言

04.字符实体(大小于号) ©(版权符号) 以及 (空格符号)所对应的实体字符都是什么?

小于号对应实体字符 ： <
大于号对应实体字符 ： >
版权符号对应实体字符 ： ©
空格符号对应实体字符 ：

05.HTML 常用标签有哪些?

HTML 常用标签包括：

- <h1></h1> ~ <h6></h6> ： 标题标签
- ： 段落标签
- ： 普通文本标签
-
 ： 换行标签
- ： 容器标签
- <img src=""> ： 图片标签
- <a href=""> ： 超链接标签
- ： 有序列表标签
- ： 无需列表标签
- <table></table> ： 表格标签

06. ECMA 标识符命名规则是什么?

第一个字符必须是字母,下划线或者美元符号($);
其他字符是数字,字母,下划线或美元符号($);
按照惯例标识符采用驼峰大小写格式,第一个单词首字母小写,其他单词首字母大写;
不能把关键字,保留字作为标识符。

07. JavaScript 中都有哪些常用数据类型?

- number 数值型
- string 字符串型
- boolean 布尔型
- undefined 未定义
- null 空
- object 对象

08. Javascript 输出的三种方式分别是什么?

控制台输出:console.log()
浏览器页面输出:document.write()
弹窗输出:alert()

09. 以下代码中,person 是什么数据类型: var person = "{name:'zhangsan',age:18}"

字符串型 string

10. Javascript 中通过 DOM 获取元素的三种方式是什么?

通过 id 获取元素:document.getElementById('id 名称')
通过标签名获取 HTML 集合:document.getElementsByTagName('标签名')
通过 class 类名获取 HTML 集合:document.getElementsByClassName('class 类名')

11. JS while 循环和 do while 循环之间的区别是什么?

do...while 循环至少执行一次
while 循环至少执行 0 次

12. JS 使用 for 循环计算 1~100 的累加和,怎样书写代码?

```
var sum = 0;
for(var i=1;i<=100;i++){
sum += i;
}
console.log(sum);
```

13. SQL 常用数据类型都有哪些?

常用的数值类型: INT,SMALLINT,DECIMAL
常用日期/时间类型: DATETIME,DATE, TIME

常用字符串类型: VARCHAR,TEXT

14. MySQL 数据的增删改查语句分别是什么?

查询语句: SELECT 字段名 FROM 库.表 [WHERE 条件 GROUP BY 字段 HAVING 条件 ORDER BY字段];
删除语句:DELETE FROM 库.表 [WHERE 条件];
更新语句:UPDATE 库.表 SET 字段 1=值 1,字段 2=值 2,字段 3=值 3 [WHERE 条件];
新增语句:INSERT [INTO] 库.表(字段 1,字段 2,字段 3...) VALUES (值 1,值 2,值 3...);

15. 创建 bookmgr 数据库，并在 bookmgr 数据库中创建 book 数据表，包含 id,book_name,author,price,publish_name 字段,并设置字段合适的数据类型与约束

```
CREATE DATABASE IF NOT EXISTS bookmgr DEFAULT CHARSET utf8;
USE bookmgr;

CREATE TABLE IF NOT EXISTS book(
id INT UNSIGNED NOT NULL AUTO_INCREMENT,
book_name VARCHAR(200) NOT NULL,
author VARCHAR(100) NOT NULL,
price DECIMAL(8,2) NOT NULL,
publish_name VARCHAR(200) NOT NULL,
PRIMARY KEY(id)
);
```

16. 在 MySQL 中的 union 是什么作用?

union使MySQL允许执行多个查询（多条SELECT语句），并将结果作为单个查询结果集返回。这些组合查询通常称为联合查询。

17. 什么是 MySQL? 它是什么类型的数据库管理系统？?

MySQL是一个开源的关系型数据库管理系统（RDBMS），它被广泛用于存储和管理结构化数据。MySQL属于关系型数据库管理系统，这意味着它使用表格（表）来组织和存储数据，表之间可以建立关系，数据存储在行和列中。

18. 在 PHP 中,常用的两种类型的数组分别是什么?特征是什么?

数值数组:带有数字 ID 键的数组
关联数组:带有指定的键的数组,每个键关联一个值

19. 怎样来获取数值数组以及关联数组的所有元素?

数值数组获取所有元素:

```
for($i=0;$i<=count($arr)-1;$i++){ echo $arr[$i] . '<br>'; }
```

关联数组获取所有元素:

```
foreach($arr as $key=>$value){echo $value . '<br>'; }
```

20. 什么是函数参数?

函数参数是在函数定义中指定的变量，用于接收函数调用时传递给函数的值。参数允许你将数据传递给函数，以便函数可以根据传递的值执行操作。

21. 在 PHP 中如何定义一个函数？

可以使用 function 关键字来定义一个函数。函数定义通常包括函数名、函数参数和函数体。以下是定义一个简单函数的基本语法：

```
function functionName(parameters) {
    // 函数体（函数的具体操作）
}
```

22. php 类中的__construct()构造函数什么时候触发?

在将类实例化为对象时,即 new 的时候自动触发__construct()构造函数

23. 怎样设置 cookie?怎样清除 cookie 中的数据?

1）设置 cookie 使用 setcookie()函数,setcookie(name,value,expire...)
name:cookie 的名称
value:cookie 的值
expire:cookie 的过期时间
2）清除 cookie:setcookie(name,value,time() - 3600)
即设置 cookie 的过期时间为一小时之前

24. 怎样设置 session?怎样清除 session?

- 使用 session 前先开启 session:session_start()
- 设置 session:$_SESSION['名称'] = 值;
- 清除 session: unset()→清除 session 文件中的数据 session_destroy()删除 session 文件

25. 每有一个人访问一次文章,浏览量加 1,使用 session 怎样完成此功能?

```
session_start();
if(isset($_SESSION['views'])){
$_SESSION['views']++;
}else{
$_SESSION['views'] = 1;
}
echo $_SESSION['views'];
```

##

16.《SQL注入 - 作者： 刘闯》

##

01. MySQL 常用字符串函数有哪些?作用都是什么?

- LENGTH(s) : 返回字符串 s 的字符数
- SUBSTR(s,n,len) : 从字符串 s 的第 n 个字符位置截取长度为 len 的字符串
- LEFT(s,n) : 截取字符串 s 的前 n 个字符
- CONCAT(s1,s2,...,sn) : s1,s2 等多个字符串合并为一个字符串
- GROUP_CONCAT() : 同一分组多个字符串合并为一个字符串
- ASCII(s) : 返回字符串 s 的第一个字符的 ASCII 码
- HEX(s) : 将字符串 s 转换为十六进制

02. MySQL 中的系统函数都有哪些,作用是什么?

- VERSION() : 返回数据库的版本号
- DATABASE() : 返回当前数据库名
- USER() : 返回当前用户
- @@DATADIR : 返回数据库路径

03. MySQL 中的其他函数

- IF(expr,v1,v2) : 如果表达式 expr 成立,返回结果 v1,否则返回 v2
- SLEEP(n) : 暂停 n 秒
- RAND() : 返回 0~1 之间的随机数
- LOAD_FILE() : 读取文件,并返回文件内容

04. order by n 意为按照第 n 个字段的值对查询结果进行排序,那么如果 order by 20 没有报 错,但 order by 21 出现报错,由此可以推断出什么结论?

- order by 20 没有报错代表数据表存在第 20 个字段,order by 21 出现报错代表数据表不存在第 21 个字段,综上可得数据表中只有 20 个字段.

05. 手工普通 SQL 注入流程共有哪几步?

- 判断是否存在注入点（字符型、数字型）
- 猜解 SQL 查询语句中的字段数
- 确定显示的字段位置
- 获取当前数据库
- 获取数据库中的表
- 获取表中的字段名
- 下载数据（拖库）

06. SQL 盲注的步骤分为哪几步?

- 判断是否存在 SQL 注入点
- 获取数据库名
- 获取数据表名
- 获取数据表中所有字段名
- 拖库(获取所有数据表中的数据)

07. 在 information_schema 元数据库的 columns 数据表中,查询数据库名(table_schema)为 news,数据表名(table_name)为 news_users 对应的所有字段(column_name),SQL 语句怎么写?

```
SELECT column_name FROM information_schema.columns WHERE table_schema='news' AND table_name='news_users';
```

08. 对于 get 型 sql 注入，如何使用 sqlmap 获取 mycms 库中 users 表中的所有数据?

```
sqlmap -u "注入点 URL 地址" -D mycms -T users --dump
```

##

16. 《WEB 应用安全 - 作者： 马志国》

##

01. 列举 OWSAP top 10， (2017 或 2021 年数据)

- 注入
- 失效的身份认证
- 敏感信息泄露
- XML 外部实体
- 失效的访问控制
- 安全配置错误
- 跨站脚本
- 不安全的反序列化
- 使用含有已知漏洞的组件
- 不足的日志记录和监控

02. 反射型 XSS 与 DOM 型 XSS 的区别

反射型 XSS 是收到服务器反射的数据在客户端浏览器执行

DOM 型 XSS 的代码执行不依赖于服务器端的数据，从客户端获取 DOM 中的数据并在本地执行

03. 通过 php 代码如何防御 XSS 攻击?

调用 htmlspecialchars()将用户输入的参数进行转义

04. 什么是 CSRF?

全称是 Cross-Site Request Forgery，中文跨站请求伪造。黑客利用已经登录的用户，诱导其访问或登录某个早已构造好的恶意链接或者页面，然后在用户毫不知情的情况下，以用户名义完成了非用户本意的非法操作

05. CSRF 的防御措施?

对于 web 用户在操作完成后，注意退出登录状态。对于开发者可以使用 csrf_token,即 使用户没有退出登录状态，也可以防止 CSRF 攻击

06. 什么是 SSRF?

服务端提供了从第三方服务器应用获取数据的功能,但又没有对第三方地址做严格过滤 与限制，导致攻击者可以传入任意的地址来让当前服务器对其发起请求,并返回目标地址 请求的数据

07. SSRF 防御措施

禁用不需要的协议，例如:仅仅允许 http 和 https 请求。

设置白名单方式。

限制请求的端口。

08. 什么是 RCE?

Remote Command/Code Execute，远程命令或代码执行。通过构造特殊的字符串，将数据 提交至 Web 应用程序， 并利用该方式执行外部程序或系统命令实施攻击，类似于SQL注入。

Web 应用程序使用了一些可以执行系统命令或代码的函数，而且对用户提交的数据过滤不严格，导致黑客可以利用服务器执行命令或代码。

09. 谈谈你对 eval 函数的理解

eval 函数的参数是字符串类型，将字符串作为 php 语句来执行。该字符串必须是合法的 php 代码,且以分号作为结束。常常作为 php 的一句话木马使用。

10. 什么是文件上传漏洞?

文件上传是 Web 应用的常见功能，允许用户上传图片、视频及其他文件类型文件。如果用户上传的是木马文件，则服务器就会收到攻击。

11. PHP 中反序列漏洞相关的魔法函数有哪些?

一般两个下划线开头的函数都是魔术方法，所谓魔术无非就是会自动调用而已:

- __construct() 当一个对象创建时被调用
- __destruct()当一个对象销毁时被调用
- __toString()当一个对象被当作一个字符串使用时被调用
- __sleep()在对象在被序列化之前运行
- __wakeup()在反序列化之后立刻被调用

12. 定义一个轿车类，有品牌和颜色属性。创建轿车对象， 并完成序列化和反序列化浏览器执行效果如下:

brand:black,color:benz
O:3:"Car":2:{s:5:"color";s:4:"benz";s:5:"brand";s:5:"black";}
object(Car)#2 (2) { ["color"]=> string(4) "benz" ["brand"]=> string(5) "black" }

```php
<?php
class Car{
var $color;
var $brand;
function __construct($color,$brand){
$this->color = $color;
$this->brand=$brand;
}
function __toString()
{
return "brand:{$this->brand},color:{$this->color}";
}
}
// 1 创建对象
$car = new Car("benz","black");
// 直接 echo 输出，自动调用__toString()
echo $car."<br>";
// 2 将对象序列化
$ser_car= serialize($car);
echo $ser_car;
echo "<br>";
// 3 反序列化
$un_car =unserialize($ser_car);
var_dump($un_car);
?>
```

13. 列出 php 文件包含函数有哪些

- include
- require
- include_once
- require_once

14. 逻辑漏洞的特点

- 与系统本身的业务功能相关，决定了逻辑漏洞的多样性

- 很难通过有规则的脚本或工具扫描发现
- 产生的流量是合法流量， 一般的防御手段和设备无法阻止
- 一般需要人工审计和手动测试发现

15. 越权漏洞的分类
- 水平越权
- 垂直越权

##
17.《渗透测试攻防实战 - 作者： 马志国》
##

01. 渗透测试报告的组成部分一般有哪些
- 封面
- 内容提要
- 漏洞总结
- 使用的工具列表
- 报告主体

02. 编写一句话木马
```
<?php @eval($_REQUEST['tedu']);?>
```

03. 列举 webshell 工具有哪些
- 中国菜刀
- 中国蚁剑
- 冰蝎

04. 根据渗透测试位置分类
- 内网渗透
- 外网渗透

05. 根据渗透测试方法分类
- 黑盒测试
- 白盒测试
- 灰盒测试

06. PTES 将渗透测试过程分为哪几个阶段
- 前期交互阶段
- 信息收集阶段
- 威胁建模阶段

- 漏洞分析阶段
- 渗透攻击阶段
- 后渗透攻击阶段
- 报告阶段

07. Web 漏洞扫描工具有哪些？

Acunetix（AWVS）：Acunetix是一款专门针对Web应用程序的漏洞扫描工具，用于发现SQL注入、XSS、CSRF等常见Web漏洞。

IBM Security AppScan：IBM Security AppScan（以前称为IBM Rational AppScan）是IBM的一个应用程序安全扫描工具，用于自动发现Web应用程序中的漏洞，包括SQL注入、跨站脚本（XSS）等。

Nessus：Nessus是一个广泛使用的漏洞扫描工具，用于检测网络和Web应用程序中的漏洞。它支持多种漏洞检测，包括SQL注入、跨站脚本（XSS）等。

OWASP ZAP：OWASP ZAP（Zed Attack Proxy）是一个免费的开源Web应用程序漏洞扫描工具，由OWASP（开放Web应用程序安全项目）维护。它提供了强大的漏洞扫描和渗透测试功能。

Burp Suite：Burp Suite是一款专业的渗透测试工具，它包含了漏洞扫描器，用于发现Web应用程序中的漏洞。它还提供代理服务器、拦截器等功能，用于手动渗透测试。

OpenVAS：OpenVAS（开源漏洞评估系统）是一个开源漏洞扫描工具，它提供了强大的漏洞检测和管理功能。

08. WebShell 管理工具有哪些？

Webshell工具常用的有：蚁剑、冰蝎、哥斯拉、Weevely。

09. RCE 漏洞利用绕过 WAF 的方式有哪些？

- 变量拼接
- 编码加密传输
- 字符替换
- 传参方式

10. SQL 注入漏洞利用绕过 WAF 的方式有哪些？

- 内联注释绕过
- 特殊字符绕过%0a
- 容器特性绕过
- WAF 性能因素绕过

11. WebShell 绕过 WAF 的方式有哪些？

- end()函数绕过

- 常量定义绕过
- 字符串拼接+双美元符号绕过
- 函数定义强行分割绕过
- 类定义强行分割绕过
- cookie 传参绕过
- 读取预定义函数绕过
- 自搭建数据库读取代码绕过
- 编码加密传输绕过
- 加密混淆

12. 安全加固中 MySQL 身份鉴别包含哪些方面？

- 默认账号：数据库系统默认普通账号或测试账号需要关闭或者删除
- 默认管理员账号：默认的管理员账号或管理测试账号需要关闭或删除，高权限账号需要控制
- 口令策略：口令的长度、复杂度、账号权限等严格按照等保或公司要求来设置
- 登录失败处理：设置登录失败的次数、等待时间等提升口令的安全，访问爆破等攻击

13. 安全加固中 MySQL 访问控制包含哪些方面？

文件权限控制：以普通权限运行数据库服务，设置属主和运行参数等；
命令历史记录保护：必要情况需要清空日志文件内容；
用户最小权限：在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限；
超时锁定：设置超时时间，在时间内没有操作，再次操作是，就会提示超时
监听本机：数据库不需要远程访问时，可禁止远程连接

14. 安全加固中如何以专门的用户账号 apache 和 apache 组运行 Apache 服务？

修改配置文件，将运行apache的用户修改为apache

```
$ sudo vim /etc/apache2/apache2.conf
User apache
Group apache
```

15. 安全加固中如何将 404 错误页面重定向，防止 Apache 信息泄露？

修改配置文件，将运行apache的用户修改为apache

```
$ sudo vim /etc/apache2/apache2.conf
# 添加如下配置
ErrorDocument 404 "<h1>Custom 404 Page</h1>"
```