六四开，把git填满

14~15个选10 每个3~4分

4~5问答题

话题：

问答题会出现这100个词，线索

**【通用】代理proxy：HTTP、SOCKS（4/5，5的优点代理域名）**

**明文GET，密文CONNECT**

**proxy**：

**代理（Proxy）是一种位于客户端和目标服务器之间的中间服务器**。

**通过代理服务器，客户端可以发送请求并获取响应，而不直接与目标服务器通信。**

代理服务器可以**提高访问速度**、**增强安全性**和**保护隐私**等方面。

proxy还可以分为**HTTP代理**与**SOCKS代理**

HTTP代理就是**专门用于通过HTTP连接**并同样通过客户端-服务器模式运行的代理；

与HTTP有所不同，**SOCKS无法读取网络数据，**不会解析或修改请求头，而是直接转发数据包。

一般用于协助与**设有防火墙且限制普通客户端访问的网站进行通信**，最重要的是，SOCKS代理可以**基于任何网络协议（HTTP、FTP、SMTP），在无论什么端口上运行，**常用于**实时通信或P2P共享等流量密集型活动，**通过**TCP**连接

**SOCKS4:**

SOCKS4是早期的版本，用于在客户端和服务器之间建立**TCP连接**。它最初设计用于支持**IPv4地址；**

**只支持连接请求**，**没有对用户进行身份验证的功能**。它的特点是简单快速，但缺乏一些安全功能，比如加密通信；

**SOCKS5**:

**SOCKS5是SOCKS协议的第五个版本**，**提供了更多的功能和安全性**。

主要特点：

**支持多种身份验证方法**，包括**无认证**、**用户名/密码认证**和 **GSS-API**（Generic Security Services Application Program Interface）认证。

**支持TCP 、 UDP ：支持更多的场景，如网络游戏等**。

**支持端口绑定功能**，可以**在代理服务器上监听指定的端口，等待外部连接并转发数据**；

**IPv6 支持**

**错误消息扩展**

**GET/POST/Connect**：

GET是**HTTP协议中的一种请求方法**，用于**从服务器获取数据**。当**使用浏览器访问网页时，通常会发送GET请求来获取页面内容**。GET请求**不会对服务器上的资源进行修改**。GET请求是**幂等**的，即**对同一资源的多个GET请求不会产生副作用；**GET**请求的参数会以查询字符串的形式附加在URL的末尾**，用于**指定请求的资源；**

POST是**HTTP协议中的一种请求方法**，用于**向服务器提交数据**，用于**在表单提交时发送数据**。

CONNECT是**HTTP协议中的一个请求方法**，通常用于**HTTP代理服务器**。当客户端希望**通过代理服务器与其他服务器建立隧道连接时**，可以使用CONNECT方法。这种方法通常用于**加密和隧道HTTP连接**，例如**HTTPS**。实现**端到端加密通信**或者**穿越防火墙进行安全通信**等；

**CONNECT的具体用法：**

客户端发送一个CONNECT请求到代理服务器，指定**目标服务器的主机名和端口号**；

代理服务器在收到这个请求后，会尝试建立与目标服务器的**TCP连接；**将客户端发送的**加密数据（GET方法返回的是明文，Connect方法返回的是密文）**通过代理服务器转发给目标服务器

**例子：**

**CONNECT example.com:443 HTTP/1.1**

**Host: example.com:443**

其中，example.com是目标服务器的主机名，443是目标服务器的端口号

代理服务器在收到这个请求后，会尝试与example.com建立TCP连接，如果连接成功，代理服务器会返回一个**HTTP 200 OK响应**，表示隧道已经建立。此后，客户端和目标服务器之间的通信流量将直接通过代理服务器进行转发，而不需要代理服务器解析或处理通信内容

**【不标准】MT proxy（telegram使用，根据应用需要订制的proxy）**

MT Proxy是一种基于Telegram Messenger的代理协议，用于帮助用户绕过网络审查和访问被封锁的网站。它采用了"Mobile Protocol"（移动协议）的简称，即**MTProto协议**，这是**Telegram专门为其通讯软件设计的一种加密协议**。

**reverse proxy：逆向代理，掩盖企业内部的网络结构，负载均衡；**

**正向代理，Aapche使用，mode proxy，写其它的也行；**

**先把网络斩断（为了安全），再加一个联通双方的proxy；**

以下是一些常见的代理类型和其功能：

**正向代理**（Forward Proxy）： 正向代理**位于客户端和目标服务器之间**，**客户端发送请求到代理服务器，然后由代理服务器转发请求到目标服务器，并将响应返回给客户端**。正向代理常用于**绕过网络限制、提高访问速度和保护隐私、隐藏客户端的真实IP地址**等方面。

**Apache HTTP服务器**可以配置为正向代理服务器，以便代表客户端访问其他服务器；

**反向代理**（Reverse Proxy）： 反向代理与正向代理相反，**位于目标服务器和客户端之间**。**客户端发送请求到反向代理，然后反向代理根据一定的规则将请求转发到目标服务器，最终将响应返回给客户端**。反向代理通常用于**负载均衡、安全性增强和隐藏服务器真实 IP 地址**等方面。

**匿名代理**（Anonymous Proxy）： 匿名代理可以**隐藏客户端的真实 IP 地址**，从而增强隐私保护。使用匿名代理时，目标服务器无法直接获取客户端的真实 IP 地址。

**【proxy奇葩用法】：（Squid软件的模块，对ssl进行中间人攻击，要求员工必须信任企业的证书，并没有破坏ssl协议）ssl\_bump，毕设演示，进来企业的数据防病毒检查（邮件zip文件很多检查很吃力，icap协议）；出去企业的数据防泄漏，检查敏感信息，根据过滤规则检查；**

**squid:**

Squid是一个**开源代理服务器软件**，主要用于**缓存Web内容并提供匿名访问、过滤内容和访问控制**等功能。

通常用作**代理服务器**，可以**提高Web服务器的访问速度**、**节省带宽**并提供一定程度的**安全性和隐私保护**。

Squid会**将访问页面的结果缓存在硬盘和内存上**，**对硬盘和内存的空间大小具有较高的要求**。

支持**HTTP，HTTPS，FTP**等服务

**ssl\_bump:**

ssl\_bump 是 **Squid 缓存服务器中一个特性**，**允许 Squid 在 HTTPS 流量中进行透明代理，以便对流量进行审查、过滤和修改**。

ssl\_bump 用于以下几个方面：

HTTPS 内容审查：Squid 可以**检查和过滤 HTTPS 流量中的内容，例如阻止恶意网站或不安全的内容**。

SSL 中间人：Squid 可以**充当 SSL 中间人，它与客户端建立加密连接，同时与目标服务器建立另一个加密连接**。可以**解密和查看 HTTPS 流量的内容，对其进行审查或修改，然后再重新加密并发送给目标服务器**。

访问控制：**ssl\_bump 可以与其他 Squid 功能结合，如 ACL**（Access Control List），从而实现**对 HTTPS 流量的访问控制**。

SSL 证书检查：Squid 可以**对客户端和服务器的 SSL 证书进行检查**，以确保 SSL 连接的安全性。

**ICAP**：

ICAP（Internet Content Adaptation Protocol）是一种**用于在网络传输过程中对内容进行动态适应和处理的协议**。

**内容过滤：** **与专门的ICAP服务器通信，对传输的内容进行过滤**，例如**实时查毒、敏感词过滤、广告拦截**等。此外，ICAP还可以根据预定义的策略**对内容进行修改或重定向**。

**压缩与优化**: ICAP可以用于对传输的内容进行压缩，**减少网络带宽占用，提高网络性能**。

**安全扫描与保护**: ICAP可用于**将传输的内容提交给专门的安全扫描服务**，以检测恶意软件、漏洞和其他安全威胁，并对受感染的内容进行处理。

透明代理: ICAP可以在网络中作为**透明代理**，对所有流经设备的内容进行**动态处理**，而无需改变终端设备的配置

**透明代理**（Transparent Proxy）： 透明代理通常**不需要客户端进行任何配置**，它在不需要客户端进行特殊设置的情况下**自动拦截并处理网络请求**。透明代理通常用于**企业网络中实施访问控制、内容过滤和监控**等方面。

**网络安全反向代理什么时候用？**

在网络安全领域中，反向代理通常用于**增强网络安全和保护后端服务器**。

以下是一些反向代理的常见用途：

**隐藏真实服务器**：通过反向代理，可以隐藏真实的后端服务器，使攻击者无法直接访问到后端服务器的IP地址和其他详细信息，从而增加了安全性。

**负载均衡**：反向代理可以作为负载均衡器，**将流量分发到多个后端服务器**上，从而减轻单个服务器的压力，提高系统的稳定性和安全性。

**SSL终结**：反向代理可以用于SSL终结，即**在反向代理服务器处对传入的加密流量进行解密，然后将未加密的流量转发给后端服务器**。这样一来，后端服务器就无需处理加密解密的操作，提高了安全性和性能。

**过滤恶意流量**：反向代理可以过滤掉一些恶意的网络流量，例如**DDoS攻击**，从而保护后端服务器免受攻击。

**缓存静态内容**：反向代理可以缓存静态内容，如**图片、CSS文件**等，从而减轻后端服务器的负担，提高网站的访问速度和安全性。

**使用sslbump破解HTTPS是怎么回事？违反了httpd的安全目标了吗？**

不违反httpd的安全目标，是员工咎由自取，需要员工手动点击信任企业的证书；

**VPN：把互联网看成不安全的场所（物理层），使用TCP/UDP/SSL连接（传输层协议），ip丢了不要紧，可以重传；**

VPN:

**虚拟专用网络（VPN）是一种安全连接方式，通过公共网络（如互联网）在远程位置之间建立私密的、加密的通信通道**。

目的是**使得远程用户或分支机构能够安全地访问组织内部的网络资源**。

VPN 可以通过多种技术实现，其中包括：

**远程访问 VPN**：远程用户通过互联网连接到组织内部的网络资源。通常使用的协议包括**PPTP（点对点隧道协议）、L2TP（层2隧道协议）和SSL/TLS（安全套接层/传输层安全）**。

**站点到站点 VPN**：用于连接两个或多个远程网络，通常用于连接分支机构和总部网络之间的安全连接。常见的协议包括**IPsec（Internet Protocol Security）和SSL/TLS**。

优点：

**安全性**

**隐藏用户的真实 IP 地址**

**远程访问、远程办公、远程维护**。

**把传输层的连接（虚拟网线两头有两个虚拟网卡【假的以太网卡，OpenVPN（走的是ssl协议）】（两种形式）：TUN/TAP模拟以太网），虚拟网线可以组建自己的网络，brctl建立网桥（交换机，802.3.4.5【只剩.3】/802.x），把它们拉在一个局域网，设置IP地址，大公司各个分部连成一个局域网，桥接可以级联，做网中网（overlay，P2P软件用，DHT【分布式路由算法】，Can/Chord，一个为了无中心通信，一个为了安全）；**

**远程桥，很多桥延伸；**

**tun(tunnel adapter)**:

**TUN（Tunnel）适配器**是**一种虚拟网络设备**，用于**在操作系统中创建网络隧道**。

这些隧道可以用于**在两个网络之间传输数据，安全性、完整性**。

**TUN适配器用于实现虚拟专用网络（VPN）的网络隧道。**

**当用户连接到VPN时，操作系统会创建一个TUN适配器，将用户的数据流量加密并通过该适配器发送到VPN服务器。VPN服务器解密数据并将其发送到目标服务器，然后将响应数据加密并返回给用户**。

**TUN适配器传输IP数据包**。

**tap(tap adapter)**:

Tap Adapter（**TAP 适配器**）是一种**虚拟网络适配器**，用于**在操作系统中创建虚拟的网络接口**。

通常**与虚拟化软件（如 VMware、VirtualBox等）一起使用**，用于**实现虚拟机与主机之间的网络通信，以及虚拟机之间的网络通信**。

用于**模拟一个完整的以太网帧**，**包括数据链路层的帧头和帧尾**。

特点：

虚拟网络：**使得虚拟机能够像真实计算机一样通过网络进行通信**，从而实现了虚拟化环境中的网络功能。

桥接网络：可以**通过桥接模式将虚拟机连接到物理网络**，使得**虚拟机可以直接与物理网络上的其他设备通信**。

隔离网络：**配置为使用私有网络或者 NAT 模式**，以**实现虚拟机之间或者虚拟机与主机之间的隔离通信**。

VPN 连接：可以**与 VPN 软件一起使用，用于建立安全的 VPN 连接，实现远程访问或者站点之间的安全通信**。

联系：

TUN 和 TAP **都是虚拟的网络设备，不对应物理硬件，而是由软件实现的虚拟接口**

TUN 和 TAP 设备都**允许用户空间应用程序和操作系统内核之间传递数据**，这使得它们非常适合于实现各种网络功能和协议栈

区别：

网络层协议支持不同：**TUN 设备工作在 OSI 模型的第三层（网络层），它传递的是 IP 数据包**。

而 **TAP 设备工作在 OSI 模型的第二层（数据链路层），它传递的是以太网帧**

适用场景不同：由于 TUN 设备传递的是 IP 数据包，因此它更适合于实现 **VPN 和其他网络隧道技术**，如 **OpenVPN**。而 TAP 设备传递的是以太网帧，因此它更适合于实现**虚拟以太网接口，如虚拟机的网桥接口**

**brctl addbr/addif**：

brctl是一个**命令行工具**，用于在Linux系统中**管理Linux内核的桥接设备**。

**brctl addbr这个命令用于创建一个新的桥接设备**：

**brctl addbr <bridge\_name>，其中<bridge\_name>是要创建的桥接设备的名称。**

示例：**brctl addbr br0** 将创建一个名为br0的新桥接设备。

**brctl addif这个命令用于向现有的桥接设备添加网络接口。**

**brctl addif <bridge\_name> <interface\_name>**

其中<bridge\_name>是要添加接口的桥接设备的名称，<interface\_name>是要添加到桥接设备的网络接口的名称。

示例：**brctl addif br0 eth0** 将接口eth0添加到名为br0的桥接设备中。

这些命令通常用于**创建和管理Linux系统中的软件交换机**，例如用于**虚拟化环境中的网络桥接和容器网络**。**桥接设备允许将多个网络接口连接在一起，以实现网络流量的转发和管理**。

IEEE 802.3：

也称为**以太网标准**，它定义了以太网的物理层和数据链路层规范。这包括了以太网的传输速率、电气特性、数据封装格式等；

**Overlay（网中网）**：

是一种网络技术，用于在现有网络基础设施之上**创建一个逻辑上的、独立于底层网络的网络**。它通常用于构建**虚拟私有网络（VPN）**、软件定义网络（SDN）、多租户网络等

特点：

**独立于底层网络**：Overlay 网络在物理网络之上创建一个逻辑层，其逻辑拓扑与底层网络的物理拓扑可以完全不同；

**隔离性和安全性**：通过 Overlay 网络，不同的用户或租户可以在同一物理网络基础设施上建立**独立的虚拟网络**，实现数据隔离和安全性。这种隔离可以通过**加密和隧道技术**来实现，确保数据在传输过程中的机密性和完整性；

**跨越多种网络技术**：Overlay 网络可以跨越多种不同的物理网络技术，包括**以太网、无线网络、互联网**等。这使得 Overlay 网络能够**在不同的网络环境中提供统一的网络服务**，实现多样化的连接需求

**扩展性和灵活性**：Overlay 网络可以**根据需求动态扩展和缩减**，**无需对底层网络基础设施进行修改**。这使得 Overlay 网络能够适应不断变化的网络需求和流量模式，提供更灵活的网络服务

**SDN 和虚拟化支持**：Overlay 网络通常与**软件定义网络（SDN）**和**网络功能虚拟化（NFV）**技术结合使用，实现对网络资源的动态编程和管理。这使得网络管理员可以通过**集中式的控制平面**对整个 Overlay 网络进行灵活的配置和管理

DHT：

即分布式哈希表（Distributed Hash Table），是一种分布式系统中常用的数据结构和算法，用于在分布式环境中管理大规模数据的分布和查找；

特点：

**分布式存储**：DHT 将大规模的数据分布式地存储在网络中的多个节点上，每个节点负责管理一部分数据的存储和查找；

**哈希映射**：DHT 使用哈希函数将每个数据项的关键字映射到一个唯一的标识符，然后根据这个标识符将数据分布到不同的节点上。常见的哈希函数有 SHA-1、SHA-256 等；

**节点路由**：DHT 使用一种称为**路由表**（Routing Table）的数据结构来管理节点之间的通信路由。每个节点都维护一个路由表，其中记录了一些节点的联系信息，以便快速地将数据请求路由到正确的节点上。通常使用分布式算法（如 **Kademlia** 等）来维护路由表，以确保节点之间的快速和有效通信；

**动态扩展**：DHT 具有良好的可扩展性，可以动态地加入和移除节点，而不影响系统的整体性能和功能。当新节点加入网络时，DHT 可以自动重新分布数据和更新路由表，以适应网络的变化；

**高效的数据查找**：通过哈希映射和路由表的支持，DHT 能够实现高效的数据查找操作。对于给定的关键字，DHT 可以通过一系列的节点路由查找到存储该数据的节点，并获取到相应的数据内容；

DHT 技术被广泛应用于分布式文件系统、**点对点网络（P2P）**、内容分发网络（CDN）、区块链等分布式系统中

远程桥（Remote Bridging）：

是一种网络技术，用于**连接两个或多个不同的局域网（LAN）**，**使它们在逻辑上表现为一个更大的LAN**。它通常用于**扩展现有的局域网**，使得跨多个地理位置的网络设备能够互相通信，同时维护各自的独立性。

远程桥的工作原理**类似于本地局域网桥接**，但它在跨越不同的地理位置进行连接。远程桥通常通过互联网或专用线路连接不同的局域网。

主要的工作流程如下：

**数据封装**: 当一个数据包从一个局域网发送到另一个局域网时，远程桥将数据包从源局域网捕获并封装成适合在远程网络上传输的格式。

**传输:** 封装后的数据包通过远程连接（如互联网）传输到目标局域网。

**解封装:** 达到目标局域网后，远程桥从数据包中提取原始数据，并将其解封装以适应目标局域网的格式。

**交付**: 解封装后的数据包被交付给目标局域网上的目标设备。

优点：

**网络扩展**

**跨地域通信**

**资源共享**

**灾备备份**

**OpenVPN替代品Wireguard（小巧）**

**OpenVPN**：

OpenVPN 是一个**开源的虚拟专用网络（VPN）解决方案**，通过**加密和隧道技术**来**创建安全的连接**，使用户能够在不安全的网络上安全地传输数据。

以下是关于 OpenVPN 的一些重要特点和工作原理：

**跨平台支持**： 适用Windows、macOS、Linux 等。

安全性： 使用 **SSL/TLS 协议**进行加密通信。

灵活性： 可以配置为**使用不同的网络协议（如 TCP、UDP）**，并支持**各种认证方法和身份验证方式（如用户名/密码、证书、双因素认证等）**。

用户可以通过 **OpenVPN 客户端软件**连接到 **OpenVPN 服务器**，并通过该连接访问远程网络资源或将其设备安全地连接到远程网络。

**Wireguard**:

WireGuard是**一种实现加密虚拟专用网络(VPN) 的通信协议和免费开源软件**

它旨在**比IPsec和OpenVPN这两种常见的隧道协议具有更好的性能和更强大的功能**；

通过**UDP传递流量**。

安全性：使用**最新的加密技术**，包括 **Curve25519、ChaCha20、Poly1305 和 BLAKE2**，以提供高级的安全性。

它的设计目标是**简化安全配置**，并在**不降低安全性的前提下提供最佳性能**。

**PPTPD，D是后缀，d是精灵的意思(好使);apache是HTTPD；**

**PPTP**：

PPTP（Point-to-Point Tunneling Protocol）和L2TP（Layer 2 Tunneling Protocol）都是用于**建立虚拟私人网络（VPN）连接的协议**，**允许远程用户通过公共网络安全地访问私有网络资源**。

PPTP：

封装机制： PPTP 使用 **GRE**（Generic Routing Encapsulation）协议来封装 VPN 数据包，从而在公共网络上进行安全传输。

加密和身份验证： 支持使用**MPPE**（Microsoft Point-to-Point Encryption）对数据进行加密，并提供了密码验证等安全机制。

**pptpd**：

PPTPd 是一个**用于 Linux 系统的 PPTP 服务器软件**，**允许在 Linux 主机上搭建 PPTP VPN 服务器，以便远程用户可以通过 Internet 访问局域网资源**；

功能特点： 提供了基本的 PPTP VPN 服务器功能，包括**允许远程用户通过 PPTP 协议连接到你的 Linux 主机，并获得访问局域网资源的权限**。

配置灵活性： PPTPd 具有一定的配置灵活性，例如**配置允许的用户、分配 IP 地址的范围、路由设置**等。

由于 PPTP 协议本身存在**安全性问题**，通常建议考虑使用更加安全和现代的 VPN 协议，如 **OpenVPN、IKEv2/IPsec** 等。

**物理网卡：ENS/ETH**

物理网卡（Ethernet，简称为**ETH**）:

是一种常见的**网络连接设备**，用于**将计算机或其他网络设备连接到局域网（LAN）或广域网（WAN）**。

它通常**以太网协议为基础**

负责**处理数据包的发送和接收**，并**管理设备与网络之间的通信**。

**每个物理网卡都有一个唯一的硬件地址，称为MAC地址，用于在网络中标识设备**。

它还可以通过**配置IP地址和子网掩码来连接到网络**，并**通过路由器或交换机与其他设备进行通信;**

**在Linux系统中，物理网卡通常以"ENS"开头**

基于系统中的**物理位置和连接顺序**进行命名,一定程度上简化了网卡的标识和管理，尤其对于**服务器等需要大量网卡的设备**来说非常有用；

**远程访问：与CS/BS区别**

**远程访问没有传结果，而是传屏幕（字符（SSH）/图形（XWindow、VNC））**

**进程、主机、客户端（X server）**

**CRT显示器，图形工作站叫X server，进程跑在隔壁主机上，像素显示在这个房间的显示器上，还有键盘鼠标，把操作传到隔壁的主机上**

**x-window**:

X Window System，简称为**X或X11**，是一种用于**图形用户界面（GUI）的窗口系统**。

它**提供了在计算机上显示和操作图形化应用程序的基础架构**。

X Window System**允许多个应用程序共享屏幕，并通过窗口管理器来管理窗口的布局和行为**。

重要信息：

**客户端-服务器模型**：**X服务器（X Server）运行在图形显示设备上，负责管理显示和用户输入设备，而图形应用程序则作为X客户端运行在X服务器之外**。

**跨平台性**： **Linux、Unix、BSD**等。

**x-server**/x-terninal:

**X Server**（X Window System Server），**负责管理图形用户界面（GUI）的显示和输入设备（如键盘、鼠标）的输入**。

它**允许用户在计算机上运行图形化的应用程序，并在屏幕上显示它们**。

**X Server通常与操作系统一起提供，并在用户登录时启动**。

X Terminal是一种**特殊的终端设备，它具有显示屏和键盘，可以连接到远程计算机上，并通过X协议显示远程计算机的图形界面**。

X Terminal本身并不运行图形化应用程序，而是作为**显示终端**，将远程计算机上的图形界面显示在其本地屏幕上。

**VNC**:

VNC是一种用于**远程桌面控制的系统**。

它**允许用户通过网络连接到远程计算机并以图形用户界面（GUI）的形式控制它**。

主要信息：

工作原理： VNC系统由**客户端和服务器端**组成。**服务器端在远程计算机上运行，并监听连接请求，而客户端则在本地计算机上运行，并发送用户输入和接收远程计算机的屏幕图像。当客户端连接到服务器时，服务器将屏幕图像发送给客户端，并且客户端将用户输入发送给服务器**。

**Linux先天不足，很多显示协议不好使、所以游戏少**

**安全：网线传字符/图形容易被偷窥，所以有SSL保护数据传输；CS结构TCP形式，如何用SSL保护安全？-L -R两个参数保护基于TCP端口的应用（安全，可以实现端口推送，VMWARE开虚拟机，同学从遥远地方连不上，使用SSL -R命令把SSH的3389端口推送到公用的服务器（都能看到的服务器）的端口（33891）当作跳板，就可以连上；端口映射，Teamviewer，云里的VPS服务器具有公网IP，都可以看见，C1把内部的端口推过去，C2就可以连上）；**

**ssh -D/-L/-R:**

这些都是**SSH命令中的选项**，用于**在SSH连接上创建不同类型的端口转发**；

-D：这个选项用于**创建动态端口转发**，也称为**SOCKS代理**。使用-D，**SSH会在本地机器上创建一个SOCKS代理服务器**，可以**通过这个代理服务器将本地计算机上的网络流量转发到SSH服务器上，从而绕过网络限制或保护你的隐私**。

例如，如果你在**某个网络中无法访问某个网站**，可以通过**-D选项将你的浏览器配置为使用SSH代理**，然后所有的网络流量都会通过SSH连接转发到SSH服务器上，最终访问目标网站。

示例命令：**ssh -D 1080 user@example.com**

SSH会在本地计算机上创建一个SOCKS代理服务器，**监听在本地端口 1080 上**，并通过SSH连接到远程服务器 example.com。你可以将本地计算机上的网络流量通过这个SOCKS代理转发到SSH服务器上，从而绕过网络限制或保护你的隐私

**-L**：这个选项用于**创建本地端口转发**。使用-L，**SSH会将本地计算机上指定端口的流量转发到SSH服务器上的另一个指定的地址和端口上**。

可以**使用本地端口转发来安全地访问远程服务器上的服务，而不必直接暴露这些服务在公共网络上**。

示例命令：**ssh -L 8080:localhost:80 user@example.com**

SSH会**将本地计算机上 localhost的 8080 端口的流量转发到远程服务器 example.com 上的 localhost的 80 端口上**。**通过访问 localhost:8080，实际访问的是远程服务器上的服务**

**-R**：这个选项用于**创建远程端口转发**。使用-R，**SSH会将SSH服务器上指定端口的流量转发到本地计算机上的另一个指定的地址和端口上**。

可以**使用远程端口转发来暴露本地计算机上的服务，从而可以从远程服务器上访问这些服务，而不必将它们直接暴露在公共网络上**。

示例命令：**ssh -R 8080:localhost:80 user@example.com**

SSH会**将远程服务器上 example.com 的 8080 端口的流量转发到本地计算机上 localhost 的 80 端口上**。**可以通过访问 lcalhost:8080 来访问远程服务器上的服务**。

TeamViewer:

是一款**远程访问**、远程控制和远程支持软件，它允许用户在不同的设备之间进行远程连接和交互

具备端到端 256-bit AES 加密、双重身份验证、跨多种操作系统和设备平台

**远程桌面连接（最常用）：安全有瑕疵，美国出口，关键场合不让用，安全强度不够，可以外挂SSL进行保护**

**WIFI：假wifi，攻击者那张图（doc中），基本的技术思路搞清楚**

Fakewifi使用**WiFi热点**实现；

Wi-Fi热点是一种无线网络技术，允许用户通过无线连接共享互联网连接。通常，Wi-Fi热点是由一台设备（通常是计算机或移动设备）创建的，允许其他设备（如智能手机、平板电脑、笔记本电脑等）通过Wi-Fi连接到该设备，并**通过该设备访问互联网**

Wi-Fi热点不安全：【**流量可被观察，流量被篡改**】

**（流量被观察）**如果Wi-Fi热点没有启用**加密技术**，例如使用**WPA2**加密，那么网络流量将以**明文形式传输**。**攻击者可以轻松截取未加密的流量，并窃取用户的个人信息、登录凭据等敏感数据；**

**（流量被篡改）**假Wi-Fi热点，欺骗用户连接；

几种流量篡改方式：

**DNS劫持**： 攻击者可以**修改用户设备的DNS设置**，**将用户的DNS请求重定向到攻击者控制的恶意DNS服务器**。通过这种方式，攻击者可以**将用户的网络流量重定向到欺骗网站或恶意网站**，使用户误以为是正常访问目标网站，从而窃取用户的信息；

**SSL/TLS劫持**： 攻击者通过**欺骗用户接受攻击者自签名的证书**来建立安全连接。一旦建立了安全连接，攻击者就可以查看和修改传输的数据，包括敏感信息；

**ARP欺骗**： 攻击者可以**发送虚假的ARP（地址解析协议）响应**，**将目标设备的IP地址映射到攻击者的MAC地址上**。这样，攻击者就可以截获目标设备和网络之间的通信流量，并对其进行篡改或监视；

**中间人攻击（Man-in-the-Middle, MITM）**： 攻击者**在用户设备和网络之间插入自己的设备**，**成为通信的中间人**。通过这种方式，攻击者可以监视、篡改或截获通信流量，包括查看、修改或窃取用户的敏感信息，如用户名、密码等



**HTTPS没用的情况：DNS劫持、假网站、IP流量被劫持【攻击者使用iptables，把用户想要访问的目标IP地址，目标端口为xx的TCP流量重定向到自己的假网站上】**

**流程：（very important）**

**建立一个假的wifi热点**

**加入DNS欺骗**【Wifi客户端通过**dhcp协议**获得ip地址和**dns服务器的ip地址**，可以**把dns的ip地址设置为自己的机器**，比如某个虚拟机中的linux，在linux中**安装一个受控的dns服务**，**当解析比如www.boc.cn的时候，给一个假的ip地址**】

**加入IP欺骗**【Linux中的iptables命令有个选项**-DNAT**，可以**重定向IP流量到某个特定的IP（自己的假网站）**】

**加入网站欺骗**【在假的IP上建立一个假冒网站，骗取用户的口令】

**考虑攻击者，假冒场景实现；**

见流程

**考虑受害者，如何判断识别假WIFI（欺骗很难，具有警惕性，有叹号就知道假的，HTTP之后有无S很重要，有S就难被骗，没有就容易被骗）；**

**确认热点身份:** 在连接到Wi-Fi热点之前，尽量确认热点的真实身份，注意Wi-Fi热点的网络名称（SSID）；

**谨慎输入个人信息**: 避免在不可信的热点上输入用户名、密码或其他敏感信息；

**检查网络安全性**：在连接到Wi-Fi热点之前，尝试了解热点的安全性设置。真实的Wi-Fi热点通常会启用加密技术（如**WPA2**）来保护网络流量，而假WiFi热点可能不会提供相同的安全保护；

**使用VPN**:使用虚拟私人网络（VPN）来**加密网络流量，帮助防止攻击者窃取敏感信息或篡改网络流量**

注意浏览器和操作系统的**安全警告**，**不要接受未知来源的SSL证书**

**假冒的WIFI能破解HTTPS中的信息吗？**

通常情况下无法直接破解HTTPS传输的信息；

HTTPS通过**TLS/SSL加密协议**对数据进行加密和认证，即使在连接到假冒的Wi-Fi热点时，由于HTTPS使用了加密保护，攻击者通常无法直接查看或篡改通过HTTPS传输的敏感信息；

即使攻击者无法直接解密HTTPS通信，他们仍然可以**监视并分析用户的网络流量**，包括**查看访问的网站、通信的频率和持续时间**等信息

攻击者可能尝试通过**欺骗用户接受自签名的SSL证书或利用中间人攻击来解密HTTPS通信**。这种情况下，**用户的浏览器可能会显示安全警告**，**但如果用户不加以注意并接受了假证书，攻击者就可以解密和篡改HTTPS通信**

**法律问题：安全要有责任（开放问题，可以问AI，多角度问法）**

**维护一个网站，有好多数据（百万级），怎么采用合适的技术和规章制度来维护网站的稳定运行？**

**根据网络安全法的规定，网站管理员应该采取哪些措施维护网站的安全？**

**例子：美国优步CSO数据被偷走，黑客勒索，CSO和黑客妥协，说发现企业的bug，然后悬赏，回收bug；撒谎被抓；**

**备份**：建立**定期备份和恢复策略，定期备份、增量备份**

**负载均衡**：针对大流量网站，使用负载均衡技术**将流量分散到多个服务器**上，以提高网站的可用性和性能

**实施访问控制**：限制对网站的访问权限，确保只有授权用户能够访问敏感信息和功能;

**网络防御**：部署**防火墙、入侵检测系统（IDS）和入侵预防系统（IPS）**等网络安全设备，以检测和阻止恶意网络流量，snort；

**proxy代理**加上对**病毒查杀**和**泄密**的过滤【**sslbump、clamav**】

**对向外走的数据进行审查【icap，sslbump**】

**Windows的域**功能“卡死一切，控制行为

努力去”**买“相关的安全软件和服务【有安全公司担保】**，有利于**规避自己的法律责任**，不要使用免费的安全软件；

企业内部建立**社工库**，给员工看看，提升警惕意识；

企业内部建立**钓鱼邮件演练系统**，假冒领导来信，让员工上当，培养员工的警惕性

监控和日志记录：设置**系统日志记录**以跟踪用户活动和潜在的安全事件；

数据**加密存储**，即使丢了攻击者也看不懂

**漏洞管理**：定期进行漏洞评估和安全审计，发现并修复网站中的潜在漏洞

网闸；

关闭没用的服务和端口；

流量监控：ntop；

蜜罐技术；

**记住几个法的名字，法条浏览一下，把握精神**

**数据丢了怎么罚？《数据安全法》**

网络安全法、数据安全法

网络安全法：

第四十条　网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条　网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意

第四十四条　任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第六十四条　网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、**没收违法所得、处违法所得一倍以上十倍以下罚款**，**没有违法所得的，处一百万元以下罚款**，**对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款**；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并**处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款**。

数据安全法：

第二十九条　开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十二条　任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

第三十六条 非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据

第四十五条　开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处**五万元以上五十万元以下罚款**，**对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款**；拒不改正或者造成**大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款**，并可以责令**暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照**，对**直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款**。

违反国家核心数据管理制度，**危害国家主权、安全和发展利益**的，由有关主管部门处**二百万元以上一千万元以下罚款**，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

第四十六条　违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

**udhcpd**

udhcpd 是一个用于 Linux 系统的**轻量级** **DHCP（动态主机配置协议）服务器软件**。

DHCP是一种**网络协议**，用于**自动分配IP地址和其他网络配置参数给连接到网络的设备**，如计算机、智能手机、网络摄像头等。

udhcpd 的主要功能是**管理和分配 IP 地址、子网掩码、网关、DNS 服务器等网络配置信**息，以便设备能够顺利地连接到网络并进行通信。

**dns有哪些安全问题？有哪些改进措施？**

DNS是互联网中用于**将域名解析为 IP 地址**的系统：

**DNS劫持**：DNS劫持是指**攻击者篡改了DNS查询结果，将用户重定向到恶意网站**。

改进措施：

使用**DNSSEC**（DNS Security Extensions）来**对DNS查询结果进行数字签名验证，**攻击者无法篡改数字签名而使其通过验证；

**DNS-over-HTTPS**（**DoH**）或**DNS-over-TLS**（**DoT**）：**将DNS查询加密在HTTPS或TLS通信中**，防止在DNS查询过程中的劫持和篡改

**多因素身份验证**：对于敏感网站和服务，建议启用多因素身份验证，以增加用户账户的安全性。即使攻击者成功劫持了用户的DNS查询，也无法绕过多因素身份验证来访问受保护的账户

**定期监控DNS设置**：网站管理员应定期监控其域名的DNS设置，以确保其未被篡改或劫持。任何不明确的变化都可能是DNS劫持的迹象，应及时采取措施纠正

**网络防火墙和安全软件**：这些工具可以监控网络流量，并及时发现异常的DNS行为；

**DNS缓存投毒**：攻击者通过**向DNS缓存中注入虚假的DNS记录**，**使得合法的域名解析到恶意的IP地址**。

**使用DNSSEC**

**限制递归查询**：DNS服务器可以限制对递归查询的响应，只允许受信任的客户端进行递归查询。这样可以**减少攻击者利用递归查询来注入虚假DNS记录的可能性**

**定期清理缓存**：定期清理DNS服务器的缓存可以**删除过期的解析记录和可能被污染的记录**，从而减少攻击者利用缓存污染攻击的机会

**随机化查询ID和源端口**：随机化DNS查询的ID和源端口可以**增加攻击者成功注入虚假DNS记录的难度**。可以**防止攻击者通过发送大量虚假DNS响应来覆盖DNS服务器的缓存**

**监控DNS流量**

**教育和意识提升**

**DDoS攻击**：DNS服务器可能成为**分布式拒绝服务（DDoS）攻击的目标**，导致服务不可用。

**缓存优化和TTL设置**：优化DNS服务器的缓存策略和TTL（生存时间）设置，**减少对DNS服务器的查询请求**，降低DDoS攻击的影响

**分布式防御系统**：部署分布式防御系统，将防护能力分布到网络各个节点，提高对DDoS攻击的抵御能力

**DNS泄漏**：由于DNS查询通常是**明文传输**的，攻击者可以通过**监听网络流量来获取敏感信息**。

使用**DNS-over-HTTPS（DoH）**或**DNS-over-TLS（DoT）**等加密协议

**防火墙和访问控制列表（ACL**）：配置防火墙和ACL以限制对DNS服务的访问，并仅**允许经过授权的用户和系统进行DNS查询**。这可以有效地阻止未经授权的访问并减少泄漏风险

**防火墙可以对包深度解析吗？**

可以，这种能力通常被称为**深度包检测**（Deep Packet Inspection，**DPI**）。

DPI不仅**检查数据包头部的信息**，还**深入检查数据包的负载部分（即数据部分）**，从而能够识别、分类和控制网络流量；

具体技术：

**协议解析**：DPI首先需要理解和解析各种网络协议。通过**解析TCP/IP协议栈**（包括应用层协议如HTTP、FTP、SMTP等），DPI可以**提取出数据包的内容，并识别数据包所携带的具体应用层数据；**

**模式匹配**：使用模式匹配技术来识别数据包中的特定内容或特征

（正则表达式匹配、字符串匹配、签名检测）

实现DPI的具体工具和框架：

**Snort**：一种开源**网络入侵检测和防御系统**，能够进行DPI并使用预定义的规则集来检测各种网络威胁。

**ngrep**：**网络抓包工具**，可以用于简单的DPI任务，通过匹配数据包内容来筛选特定流量

**Bro/Zeek**：一种强大的**网络分析框架**，能够进行复杂的DPI和流量分析

**考一道AI和安全的题目，给一个示例题目；**

简述人工智能在网络安全中的三种主要应用场景，并举例说明每种应用场景的具体应用。

**威胁检测和响应**：使用机器学习算法来分析网络流量并检测异常行为

**恶意软件检测**：使用深度学习模型来分析文件特征并判断文件是否为恶意软件，使用**卷积神经网络（CNN）**分析文件的二进制特征或使用**递归神经网络（RNN）**分析文件的动态行为

**身份验证和访问控制**：利用AI技术对用户的面部特征进行识别和匹配，以确保只有授权用户才能访问敏感系统

**如果考一道llama模型和网络安全的题目，给一个示例的题目；再给个答案；**

LLaMA模型是一种**基于Transformer架构的大规模语言模型**，在各种NLP任务中表现出色；

题目一：讨论LLaMA模型在网络安全中的两种潜在应用场景，并举例说明每种场景的具体应用

**网络钓鱼检测**：使用LLaMA模型分析电子邮件内容，识别网络钓鱼攻击。通过**训练LLaMA模型识别钓鱼邮件的常见特征**（如紧急语气、可疑链接等），可以自动标记和过滤潜在的钓鱼邮件，保护用户免受攻击

**自动威胁情报分析**：使用LLaMA模型分析网络安全报告、威胁情报数据和日志文件。例如，LLaMA可以自动提取和总结大量的威胁情报报告，帮助安全团队快速了解最新的攻击趋势和威胁情报

题目二：LLaMA模型在网络安全应用中可能面临的安全风险及缓解措施

LLaMA模型可能面临**对抗性攻击**，**攻击者可以生成对抗性文本，使得模型产生错误的输出**。例如，通过**插入无害但巧妙设计的文本片段，攻击者可能误导模型对钓鱼邮件或恶意内容的识别**

缓解措施：实施**对抗性训练和模型增强技术**。通过**在训练过程中引入对抗性示例**，使模型在面对对抗性攻击时能够更稳健；