1. **你在工作中接触过挖矿病毒吗，如何判断电脑是否感染了挖矿病毒？**

电脑被挖矿的特征：

1、电脑变得异常缓慢，频繁无响应、网络卡顿、风扇异响，反复重启等问题，排除系统和程序本身的问题后重启依然无法恢复，就需要考虑是否感染了“挖矿”木马病毒了；

2、中了挖矿木马，因为会在系统中运行挖矿程序，使得计算机在正常运行下会变得非常卡顿，并且CPU的使用率会变得非常高，甚至会达到100%；

3、网络流量变大；

4、耗电量急剧上升。

1. **做的哪方面的应急 ，挖矿病毒的应急思路 （重点）**

从内网DNS服务器、流量审计等设备获取恶意域名，利用获取的域名和微步等威胁情报平台确定挖矿木马种类，排查 CPU、内存、网络等占用情况，获取异常进程 PID，根据 PID 可以获取进程的详细信息，获得详细信息后可以对恶意文件样本进行采样，对恶意进程进行查杀，删除恶意文件，对系统的计划任务、启动项、账号等可能被攻击者隐藏后门的位置进行排查。

1. **后渗透集权系统**

后渗透时常见的对集权系统的攻击就是针对域控的攻击，我们进入内网后可以尝试在内网的机器上进行密码的抓取，如果可以抓取到域管的密码或者hash就可以利用抓到的信息登录域控，获得域控权限后即可尝试导出域内所有用户的hash，实现对于整个域环境的控制。

1. **权限维持的方法**

创建隐藏账号、利用启动文件夹或者注册表添加自启动项、注册成服务进行自启动、利用计划任务特定时间执行程序、利用Winlogon Helper、IFEO注入等方式都可以进行权限维持

1. **linux系统提权方式 （重点）**

1）利用系统内核漏洞提权、可以根据系统内核版本号查找提权EXP 进行利用

2）利用 SUID 提权，如果 vim、find、bash、cp、mv、awk等命令具有SUID权限时可尝试利用提权

3）计划任务提权，大概思路就是，有root权限的计划任务权限配置不当，使我们普通用户也拥有修改权限，我们可以修改其中的内容，使之提权成功。

1. **内网渗透了解吗？聊一聊内网渗透的思路 （重点）**

进入内网后先进行信息收集，探测内网中的存活主机，收集用户信息、主机信息、网络信息等内容，尝试获取各类凭据信息（部分操作需要提权）。通过搭建代理使我们可以访问目标内网，可以对内网中存在的web服务、数据库等进行攻击，然后使用收集到的用户密码和hash等信息进行横向移动，逐步拿到域控权限，然后留后门进行持久化控制即可。

1. **拿下系统后有没有做横向**

有做横向，拿下系统后做内网的信息收集，看内网当中有哪些存活的机器，以及这些机器开放的端口，看看有没有一些存在漏洞的服务。也可以尝试收集一些用户凭证信息，比如操作系统的账号密码、常用的软件（例如mstsc、xshell、navicat、各类浏览器）中保存的用户名和密码，利用收集到用户名、密码、hash等信息结合计划任务、psexec、wmi等进行横向移动了。

1. **在内网渗透中，通过钓鱼邮件获取到主机权限，但是发现内网拦截了tcp的出网流量，聊一下这个时候应该怎么进行通信？ （重点）**

从提出的问题来看，应该只是拦截了直连 TCP 的出网流量，要不然怎么获取到主机权限，除非冲锋马是 DNS 通信。那么我们就直接以 HTTP/HTTPS 进行通信即可。

1. **命令执行漏洞，http不出网有什么比较好的处理方法，接上一题，通过隧道通信，详细讲讲通过什么类型的隧道，讲讲具体操作 （重点）**

可以通过ICMP隧道进行通信，具体操作如下

1. 在攻击机上执行 sysctl -w net.ipv4.icmp\_echo\_ignore\_all=1 关闭ICMP应答，防止接受本地的响应的ping数据包。
2. 将pingtunnel上传至web服务器后执行 ./pingtunnel -type server -noprint 1 -nolog 1命令，即可在 Web 服务器开启服务器端监听。
3. 在攻击机执行 ./pingtunnel -type client -l :1080 -s 跳板机IP -sock5 1命令连接服务端，这里表示设置本地的 1080 端口作为SOCKS连接端口。
4. 在攻击机中修改 proxychains4.conf 配置文件，并在其底部添加一行 socks5 127.0.0.1 1080 参数来我那次 ProxyChains 代理设置。
5. 配置完成 ProxyChains 后即可使用，proxychains 命令 来使用建立的ICMP隧道了
6. **说一下bypass uac 是什么**

UAC是Windows操作系统中的一项安全功能，限制未经授权的应用程序和操作对系统资源的访问和修改，他会要求用户确认或提供管理员权限来减少潜在的恶意操作。bypass uac 就是使用非 administrator 的管理员用户绕过uac限制，使其不弹出UAC提示框就可以做一些管理员才能做的事情，可以通过修改白名单程序的注册表、劫持dll等方式来实现

1. **向日葵漏洞**

可以利用bypassuac的方式运行运行向日葵远程控制软件，然后老版本可以直接从配置文件或者注册表中读取向日葵连接密码。新版本需要利用procdump来导出向日葵的内存信息，然后从内存信息中获得识别码和连接密码，从而实现远程控制，todesk也能用这种方法来获取连接信息。