应急响应之畸形的爱

应急响应场景挑战说明手册

一，赛前环境准备

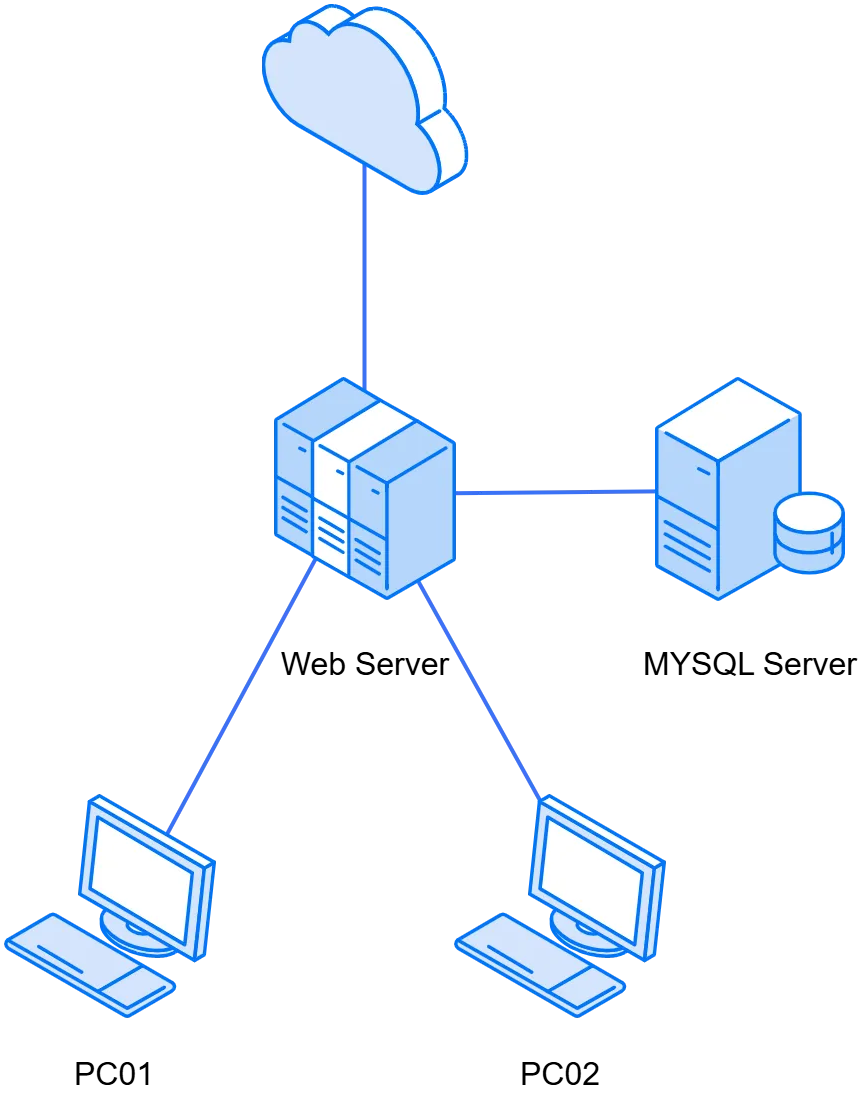
系统Windows10/Windows11（不支持armWindows、Linux、MacOS）

选手通过解压密码：进行解压

压缩包采用7z高压缩算法，请选手使用最新版7Zip进行解压

https://www.7-zip.org/

二，网络拓扑



三，资产清单

主机名	操作系统登录	服务登录
WebServer	root/root	webserver/webserver
SQL服务器	sql/sql	
Windows7 PC 1	administrator/wmx666	

Windows10 PC2	administrator/zjl@123	

四，答题说明

1.应急响应模块采用本地解题，线上提交的答题模式。

2.根据答题平台中应急响应题目的题目要求，在本地进行解题，获取到flag后，提交到答题平台。

3.CTF 模块与急响应模块都需提交Writeup，请各参赛选手以战队为单位，在竞赛结束后6小时内在答题平 台提交。

五，注意事项

1.应急响应环境为本地环境，需要提前在网盘进行下载。

2.本地环境的压缩包密码将会在开赛前一小时公布，选手需提前部署环境。

3.应急响应环境占用空间较大，需要为存放环境的目录至少预留300G的磁盘空间。

4.应急响应环境需要同时开启8台虚拟机，占用配置较高，推荐电脑配置至少8核16G。

5.禁止在竞赛过程中对提供的账户密码进行修改，以免造成服务不可用。

6.推荐在环境部署完毕的情况下创建一次快照，出现意外可立即恢复快照以节省时间。

六，部署流程

（一）安装Vmware虚拟机（如已安装可跳过） 1.从以下链接 https://www.vmware.com/go/getworkstation-win 下载 VMware Workstation 17。 2.按照安装提示安装VMware Workstation

（二）虚拟机网络配置

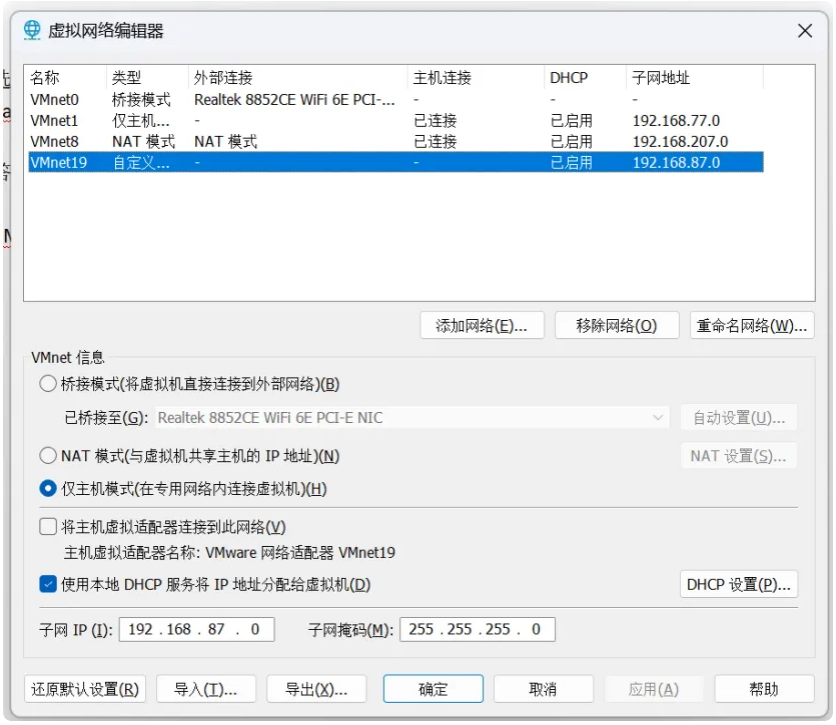
1.在VMware 主界面右上角点击“编辑”，打开“虚拟网络编辑器”

2.在打开的界面中点击“更改设置”。

3.选中“虚拟网络编辑器”中的NAT模式网卡，修改下方的子网IP和子网掩码

添加网络VMnet19 仅主机模式

设置子网ip192.168.87.0 255.255.255.0


虚拟网络编辑器
名称 类型 外部连接 主机连接 DHCP 子网地址
VMnet0 桥接模式 Realtek 8852CE WiFi 6E PCI-... - - -
VMnet1 仅主机... - 已连接 已启用 192.168.77.0
VMnet8 NAT 模式 NAT 模式 已连接 已启用 192.168.207.0
VMnet19 自定义... - - 已启用 192.168.87.0
添加网络(E)...
移除网络(O)
重命名网络(W)...
VMnet 信息
桥接模式(将虚拟机直接连接到外部网络)(B)
已桥接至(G): Realtek 8852CE WiFi 6E PCI-E NIC
自动设置(U)...
NAT 模式(与虚拟机共享主机的 IP 地址)(N)
NAT 设置(S)...
仅主机模式(在专用网络内连接虚拟机)(H)
将主机虚拟适配器连接到此网络(V)
主机虚拟适配器名称: VMware 网络适配器 VMnet19
使用本地 DHCP 服务将 IP 地址分配给虚拟机(D)
DHCP 设置(P)...
子网 IP (I): 192 . 168 . 87 . 0
子网掩码(M): 255 . 255 . 255 . 0
还原默认设置(R)
导入(T)...
导出(X)...
确定
取消
应用(A)
帮助