第二届“Parloo”CTF应急响应挑战赛

应急响应场景挑战说明手册

一，介绍

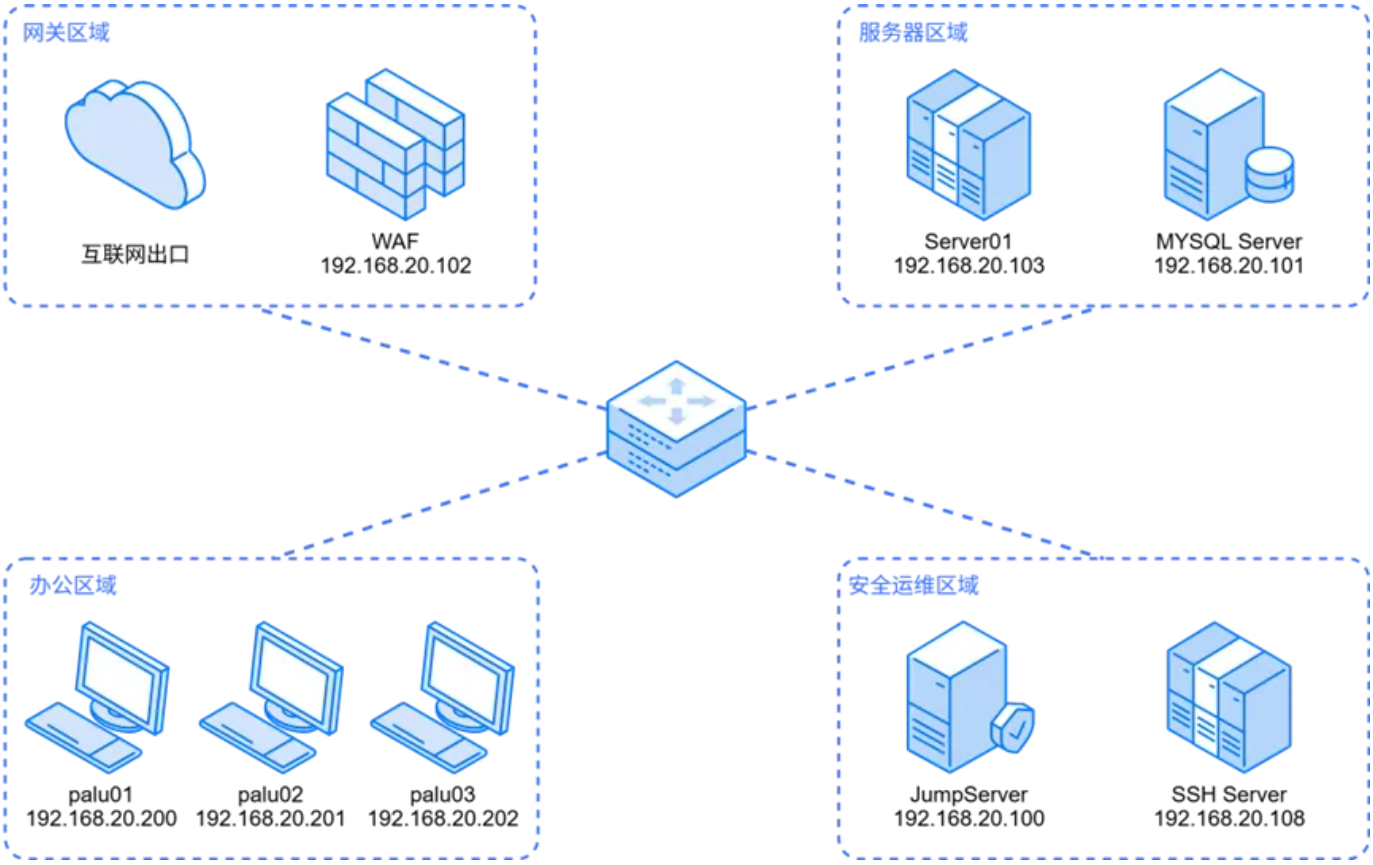
欢迎大家再次相聚于“信息安全探索之旅”的盛大开幕式。在过去的一年里，我们共同经历了无数挑战与机遇，始终在数据安全的海洋中乘风破浪。如今，随着科技的迅速发展和网络威胁的日益复杂，信息安全的重要性愈发凸显，成为了我们每一个人、每一个单位不可或缺的责任。

在这一全新的旅程中，我们将继续扮演勇敢的探险者，深入信息系统的各个角落，寻找潜藏的风险与挑战。我们的目标是更加全面地识别潜在的威胁，增强团队的安全意识，确保每一份珍贵的信息资产都能安全无虞。在这次航行中，我们不仅要面对数据泄露、非法入侵和恶意攻击这些显而易见的危险，更要关注日益增多的物联网安全隐患。

为了应对这些风浪，我们将充分利用先进的技术手段，建立更为坚固的信息防护体系。通过全方位的风险评估和应急响应机制，我们将锻造出一副更为强韧的铠甲，提升航行的安全性和稳定性。

让我们携手并肩，迎接这次“信息安全探索之旅”的新篇章。每个人都是这场旅程中不可或缺的一环，您们的参与和努力将是我们成功的关键。让我们一起努力，确保我们的信息系统如同最强大的舰队，勇往直前、无畏无惧，驶向更安全的未来！

二，网络拓扑



三，资产清单

区域	主机名	IP地址	操作系统登录	服务登录
安全运维区域	JumServer	192.168.20.100	ubuntu/ubuntu	http://192.168.20.100/ admin/Skills@2020
	sshServer	192.168.20.108	ubuntu/Skills@sshserver	

服务器区域	Server01	192.168.20.103	ubuntu/Skills@server	http://192.168.20.103:16303/9bbe149955 c394c5de46/e36c392092 http://192.168.20.102:3000/ admin@qq.com/未知
	Mysql	192.168.20.101	ubuntu/Skills@mysql	http://192.168.20.101:20221/4a883f0c56 64a44f8137/f8941f8eb7 root/mysql_QPiS8y
网关区域	Waf	192.168.20.102	ubuntu/Skills@waf	https://192.168.20.102:9443/ admin/VF6NXMs7
办公区	palu01	192.168.20.200	Parloo/Skills@01	
	palu02	192.168.20.201	Parloo/Skills@02	
	palu03	192.168.20.202	Parloo/Skills@03	此靶机为"近源"对应靶机

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

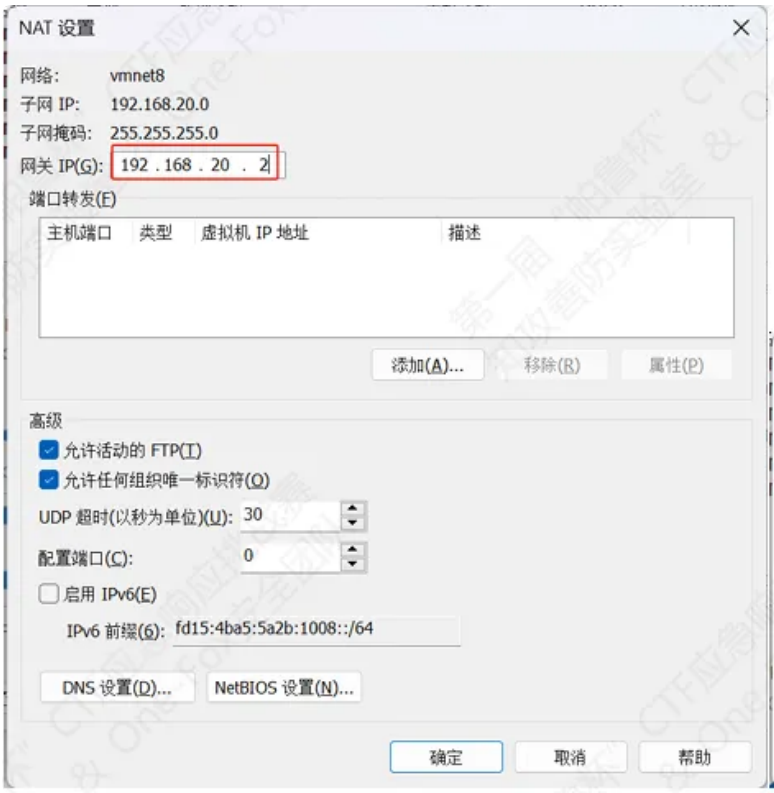
（二）虚拟机网络配置

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

4.按照下方图片修改NAT模式网卡的“NAT设置”和“DHCP设置”。

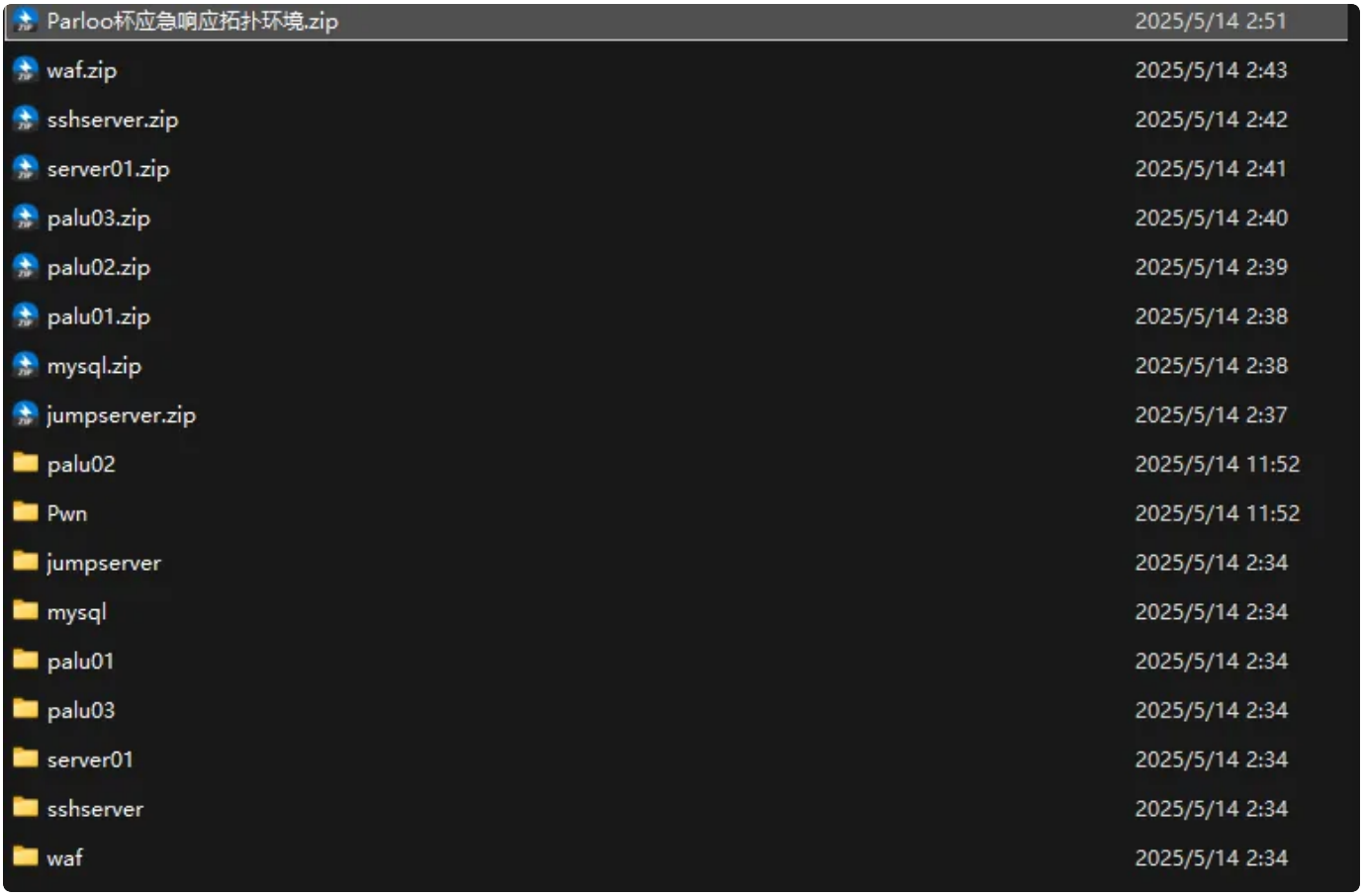


5.修改完成后点击“虚拟网络编辑器”下方的确定完成网络配置。

（三）导入虚拟机

[提供ovf和vmx两种导入虚拟机的方式，可自行选择喜欢的方式导入，仅需下载一种方式的压缩包，使用一种方式部署即可] 导入vmx虚拟机

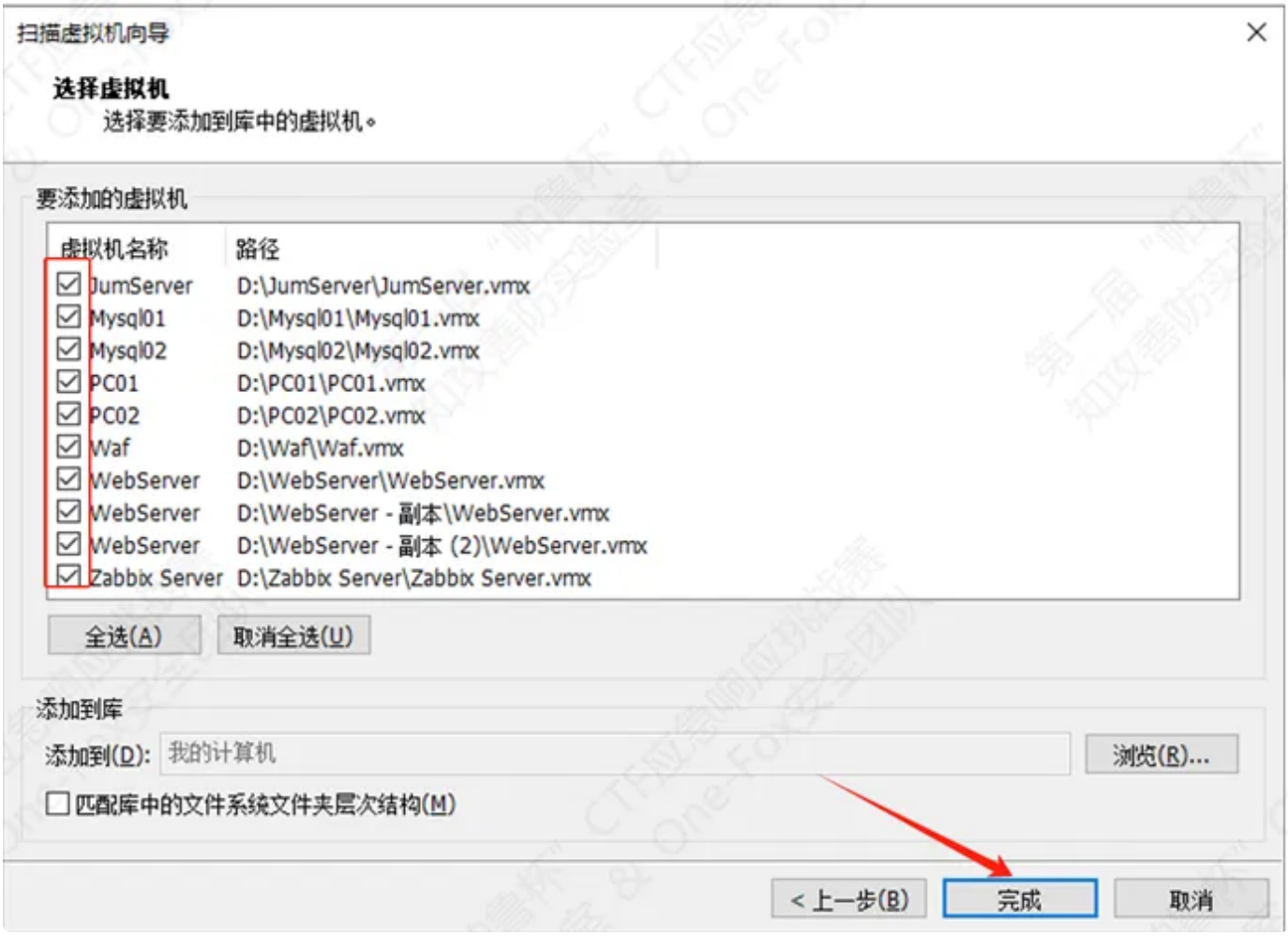
1.选择vmx格式的压缩包进行下载，下载完成后根据公布的压缩包密码进行解压，并将解压出来的所有 虚拟机放置在同一目录中。



2. 点击虚拟机主页面右上角“文件”，点击扫描虚拟机。

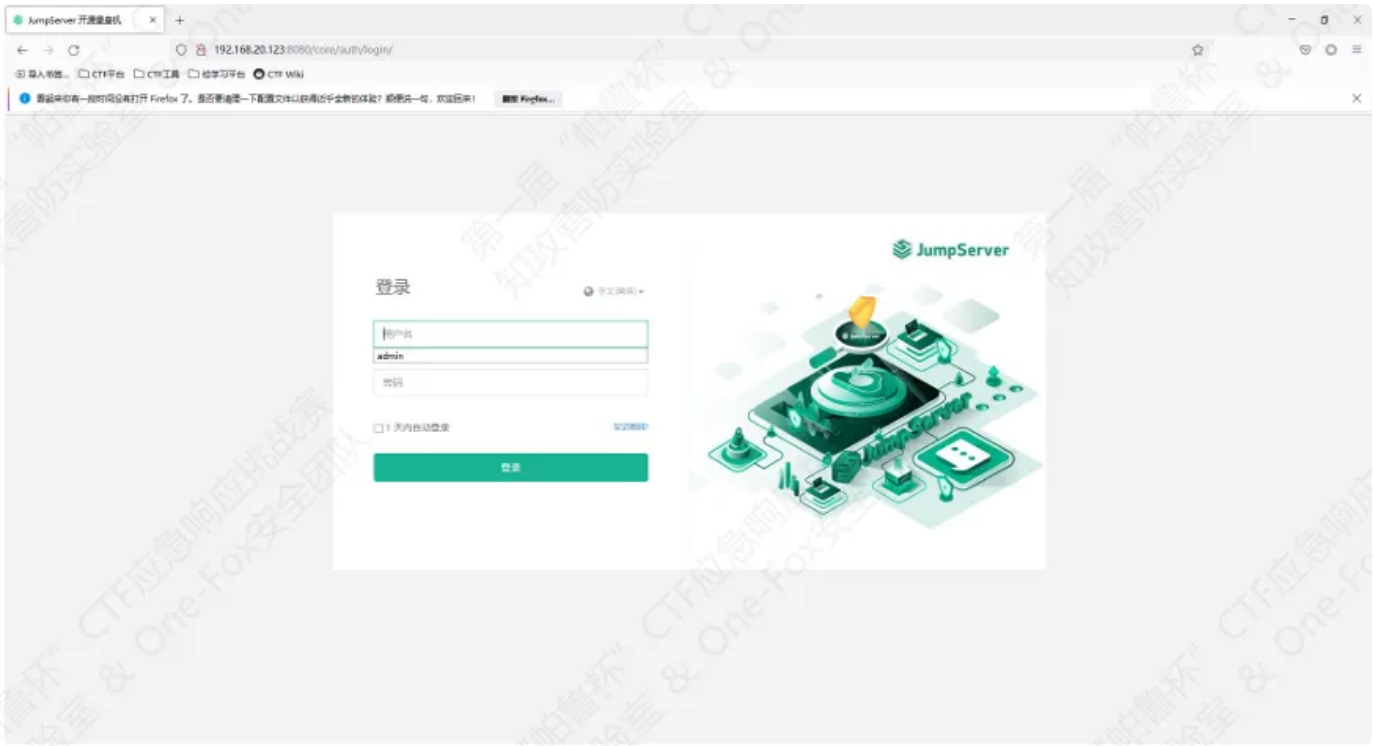
3.在“扫描的位置”处选择解压出来的虚拟机文件目录。

4.点击下一步，在之后的界面选定环境所需要的8台虚拟机，点击完成创建。



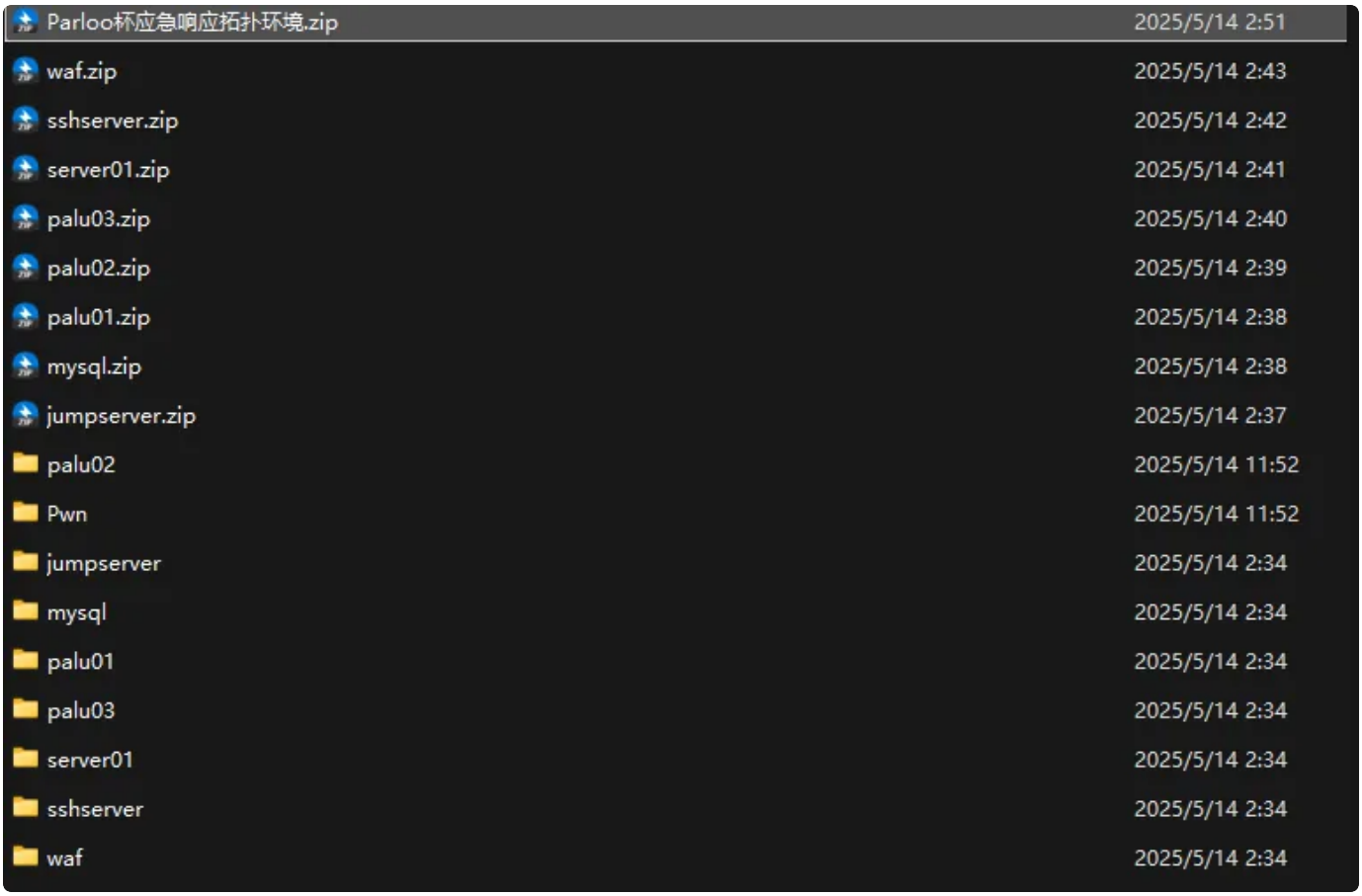
5.确保虚拟机设置当中网卡选择NAT模式，完成修改。

6.启动环境中所需的全部虚拟机，测试连通性正常后完成配置。



导入ovf虚拟机

1.选择ovf格式的环境压缩包进行下载，下载完成后根据公布的压缩包密码解压，将解压出来的所有虚 拟机放置在同一目录中。



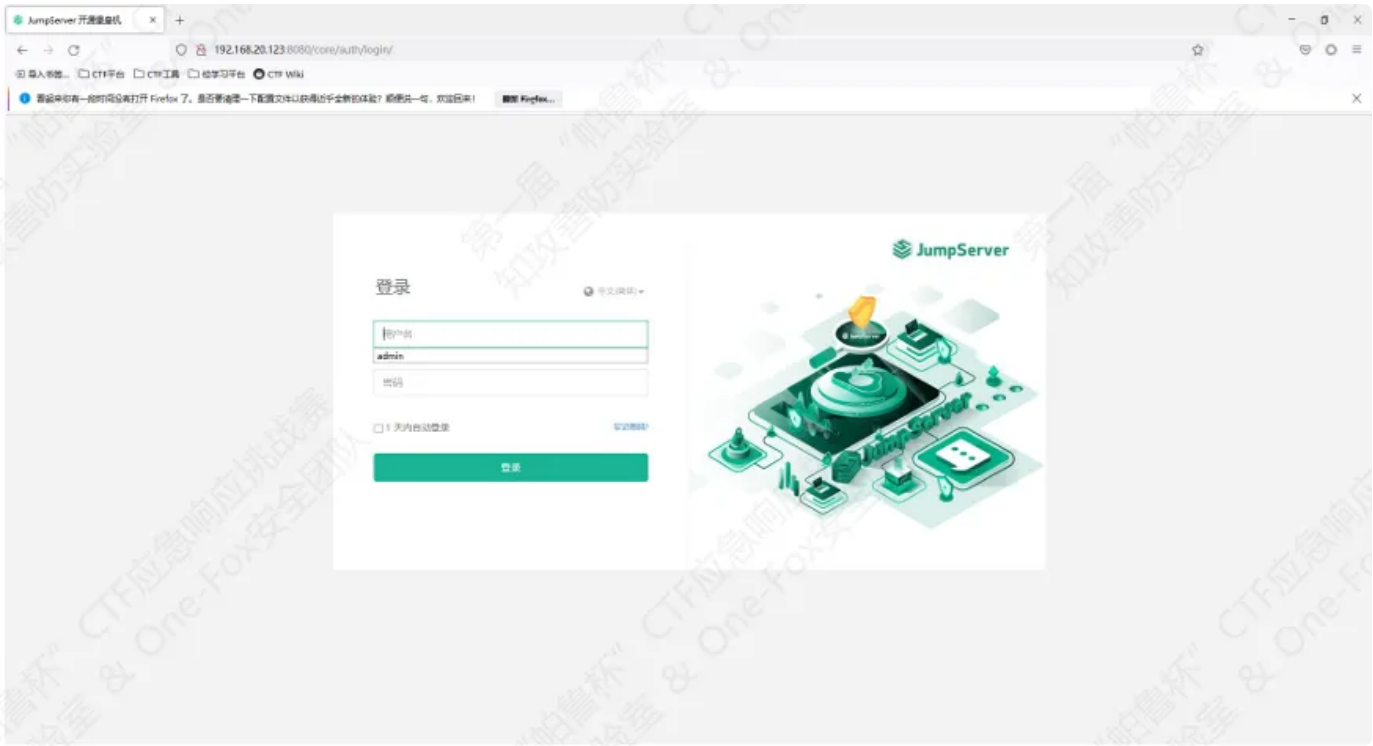
2.选择每台虚拟机目录中的.ovf文件，双击或者拖入Vmware虚拟机中，出现“导入虚拟机”界面。

3.在打开的“导入虚拟机”中输入正确的主机名，选择空间充足的存储路径，点击 “导入”完成导入 操作。

4.按照步骤3的方法，把环境中提供的8个虚拟机文件都进行导入。

5.确保虚拟机设置当中网卡选择NAT模式，完成修改。

6.启动环境中所需的全部虚拟机，测试连通性正常后完成配置。


JumpServer 开源堡垒机
192.168.20.123:8080/core/auth/login/
CTF平台
CTF工具
CTF Wiki
登录
admin
登录
JumpServer