

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

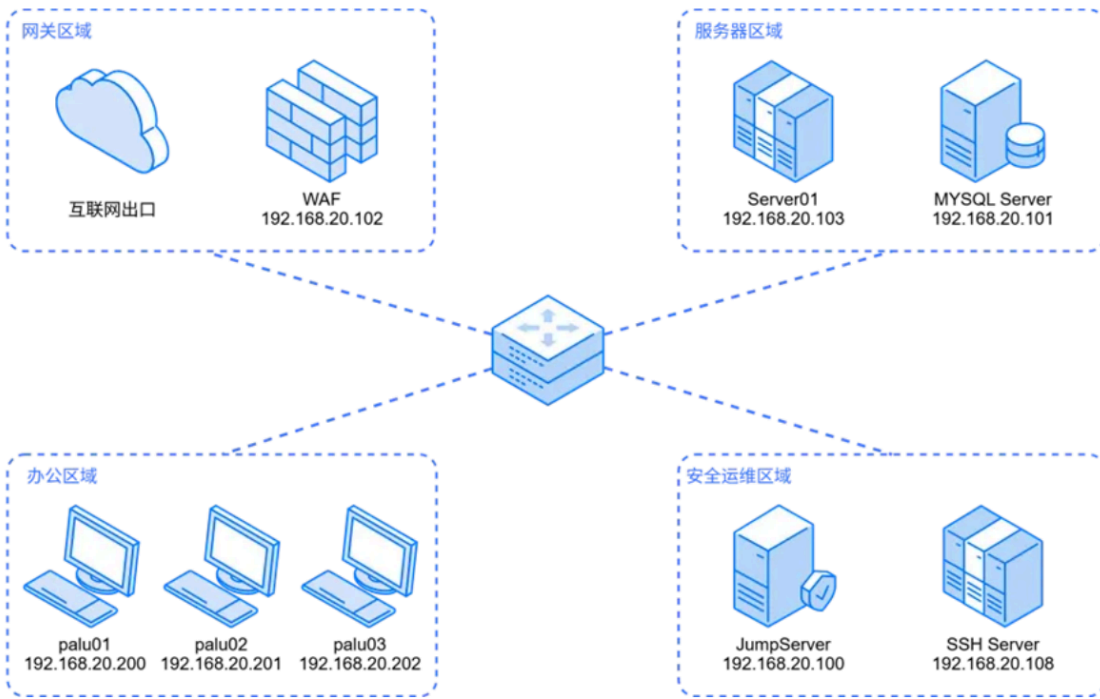
欢迎大家再次相聚于“信息安全探索之旅”的盛大开幕式。在过去的一年里，我们共同经历了无数挑战与机遇，始终在数据安全的海洋中乘风破浪。如今，随着科技的迅速发展和网络威胁的日益复杂，信息安全的重要性愈发凸显，成为了我们每一个人、每一个单位不可或缺的责任。

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

主机名	IP 地址	操作系统登录	服务登录
JumpServer	192.168.20.100	ubuntu/ubuntu	http://192.168.20.100/ admin/Skills@2020

主机名	IP 地址	操作系统登录	服务登录
sshServer	192.168.20.108	ubuntu/Skills@sshserver	
Server01	192.168.20.103	ubuntu/Skills@server	http://192.168.20.103:16303/9bbe149955c394c5de46/e36c392092 http://192.168.20.102:3000/ admin@qq.com /未知
Mysql	192.168.20.101	ubuntu/Skills@mysql	http://192.168.20.101:20221/4a883f0c5664a44f8137/f8941f8eb7 root/mysql_QPiS8y
Waf	192.168.20.102	ubuntu/Skills@waf	https://192.168.20.102:9443/ admin/VF6NXMs7
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模块与应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VMwareWorkstation17。2.按照安装提示安装VMwareWorkstation
- (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”。

NAT 设置

网络: vmnet8
子网 IP: 192.168.20.0
子网掩码: 255.255.255.0
网关 IP(G): 192.168.20.2

端口转发(E)

主机端口	类型	虚拟机 IP 地址	描述
------	----	-----------	----

添加(A)... 移除(R) 属性(P)

高级

☒ 允许活动的 FTP(F)

☒ 允许任何组织唯一标识符(O)

UDP 超时(以秒为单位)(U): 30

配置端口(C): 0

☐ 启用 IPv6(E)

IPv6 前缀(G): fd15:4ba5:5a2b:1008::/64

DNS 设置(D)... NetBIOS 设置(N)...

DHCP 设置

网络: vmnet8
子网 IP: 192.168.20.0
子网掩码: 255.255.255.0
起始 IP 地址(S): 192.168.20.128
结束 IP 地址(E): 192.168.20.254
广播地址: 192.168.20.255

天: 小时: 分钟:

默认租用时间(D): 0 0 30

最长租用时间(M): 0 2 0

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。

名称	类型	主机连接	虚拟机连接	DHCP	子网地址
VMnet0	自定义...	-	-	-	192.168.29.0
VMnet1	仅主机...	-	已连接	已启用	192.168.146.0
VMnet2	桥接模式	Realtek USB GbE Family Cont...	-	-	-
VMnet8	仅主机...	-	已连接	已启用	192.168.20.0
VMnet10	自定义...	-	-	-	192.168.101.0
VMnet14	仅主机...	-	已连接	-	10.10.210.0

添加网络(E)... 移除网络(Q) 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): 自动设置(U)... NAT 设置(S)...

☐ NAT 模式(与虚拟机共享主机的 IP 地址)(N)

☒ 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 VMnet8

☒ 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): 192.168.20.0 子网掩码(M): 255.255.255.0

还原默认设置(B) 导入(I)... 导出(X)... **确定** 取消 应用(A) 帮助

Parlool杯应急响应拓扑环境.zip	2025/5/14 2:51
waf.zip	2025/5/14 2:43
sshserver.zip	2025/5/14 2:42
server01.zip	2025/5/14 2:41
palu03.zip	2025/5/14 2:40
palu02.zip	2025/5/14 2:39
palu01.zip	2025/5/14 2:38
mysql.zip	2025/5/14 2:38
jumpserver.zip	2025/5/14 2:37
palu02	2025/5/14 11:52
Pwn	2025/5/14 11:52
jumpserver	2025/5/14 2:34
mysql	2025/5/14 2:34
palu01	2025/5/14 2:34
palu03	2025/5/14 2:34
server01	2025/5/14 2:34
sshserver	2025/5/14 2:34
waf	2025/5/14 2:34

(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。

然后就行了 扫描你的那个目录，导入就行