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/





三,资产清单

主机名	操作系统登录	服务登录
WebServer	root/root	webserver/webs erver
SQL服务器	sql/sql	
Windows7 PC 1	administrator/w mx666	

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"

🔁 Palu	CTF -	VMware Worl	kstation												
文件(F)	编辑	(E) 查看(V)	虚拟机(M)	选项卡(T)	帮助(H)		•	무	Ø	E	9		8	>_	p
库 の在は		剪切(T) 复制(C) 粘贴(P)	/	Ctrl+X Ctrl+C Ctrl+V) PaluCTF	×		1	A d	a B	N.				2
E L S	•	虚拟网络编辑器 首选项(R)	봅(N)	Ctrl+P	机设置										

2.在打开的界面中点击"更改设置"。

2 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	自定义		2 · · · · · · · · · · · · · · · · · · ·	-	192.16	8.29.0
/Mnet1	仅主机	•	已连接	已启用	192.16	8.146.0
/Mnet2	自定义	· ////	1.	-	192.16	8.8.0
/Mnet8	NAT 模式	NAT 模式	已连接	已启用	192.16	8.100.0
/Mnet10	自定义	- 1987 A	19/-	-	192.16	8.101.0
VMnet14	仅王机		已连接		10.10.	210.0
		T AT	添加网络(<u>E)</u>	移除阿	网络(<u>Q</u>)	重命名网络(W).
/Mnet 信息	H-11/12 He for tu					
0 桥接住	奥式(舟)虚拟机	且按注接到外部网络)(世)				
已桥	接至(G):				\sim	自动设置(U)
O NAT	模式(与虚拟机	1共享主机的 IP 地址)(<u>N</u>)				NAT 设置(<u>S</u>)
O 仅主机	N模式(在专用	网络内连接虚拟机)(出)				
 将主机 主机) 	几虚拟适配器; 虚拟适配器名;	套接到此网络(⊻) 称:				
使用2	^{本地} DHCP 服	务将 IP 地址分配给虚拟机(D)				DHCP 设置(P)
-	I): 192 .16	8,29.0 子网掩码()	<u>()</u>): 255 , 255 , 255 , 0	0		
子网 IP (
子网印(▲ 需要具备管理员	寺权才能修改	如《外配置》	。 💔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

白朴	类型	外部连接	主机连接	DHCP	子网地	址
VMnet0 VMnet1	桥接模式 収主和	Realtek 8852CE WiFi 6E PCI	- 已连接	- 戸白田	- 192.16	8 77 0
VMnet8	NAT 模式	NAT 模式	已连接	已启用	192.16	8.207.0
VMnet19	自定义		-	已启用	192.16	8.87.0
			添加网络(E)	移除网	网络 <mark>(O</mark>)	重命名网络(W
VMnet 信息	1					
○桥接樹	莫式(将虚拟机	直接连接到外部网络)(B)				
已桥	接至 <u>(G</u>): Rea	Itek 8852CE WiFi 6E PCI-E NIC			\sim	自动设置(<u>U</u>)
		1 # ᄒ ᅷ ᄳ ᅘ TO +바비 \/\\)				NAT 设置(S)
	模式(与虚拟制	1.共享土机的 IP 地址/(N)				
○ NAT 7	模式(与虚拟制 1.模式(在专用	(共享主机的 IP 地址)(<u>N</u>) 网络内连接虚拟机.)(H)				
○ NAT 7 ○ 仅主札	模式(与虚拟村 几模式(在专用	レ共享主机的 IP 地址)(№) 网络内连接虚拟机)(<u>H</u>)				
 NAT; 	模式(与虚拟材 几模式(在专用 几虚拟适配器) 表拟活融器2	1大学主机的 IP 地址(<u>(M</u>) 网络内连接虚拟机)(<u>H</u>) 主接到此网络(<u>V</u>) 称: VMwaro 网络活動器 VMact10				
 NAT; 仅主机 将主机 主机, 	模式(与虚拟材 U模式(在专用 U虚拟适配器; 虚拟适配器名	(H-手上がは) IP JB/L/(N) 网络内连接虚拟机)(出)				
 NAT; Q主机 将主机 主机, 使用2 	模式(与虚拟机 几模式(在专用 几虚拟适配器; 虚拟适配器名 *地 DHCP 服	(共享土がほり IP JB/LT/(<u>N</u>) 网络内连接虚拟机)(<u>H</u>) 主接到此网络(<u>V</u>) 称: VMware 网络适配器 VMnet19 务将 IP 地址分配给虚拟机(<u>D</u>)				DHCP 设置(P)
 NAT; 仅主机 将主机; 学使用本 子网 IP (模式(与虚拟机 几模式(在专用 几虚拟适配器; 虚拟适配器名 本地 DHCP 服 I): 192.16	(共享土も(出) IP JB/L7(N) 网络内连接虚拟机)(出) 主接到此网络(V) 称: VMware 网络适配器 VMnet19 务将 IP 地址分配给虚拟机(D) 8、87、0 子网推码(M):	255 . 255 . 255 . ()		DHCP 设置(P)