第3章

故障排查

终端在运行过程中,由于应用复杂性和攻击多样性,往往表现出不同的特征。这些特征可能隐藏于网络流量、系统进程、动态链接库、应用程序等各种系统组件中,如何将这些特征从庞大的组件信息中提取出来,用于解决相应的故障现象、安全问题,需要用到一些特定的工具来提取这些特征。

本章主要学习终端安全管理系统常见的故障排查工具的使用方法,用于检查、监控包括网络、进程、应用在运行过程中,如何对系统的资源进行调用、数据的流向、用户权限的管理和调用等方面的内容。对于实际工作中遇到的问题,使用此类工具也可以获得比较好的分析效果,对于了解和掌握解决问题的方法非常有帮助。

3.1 网络流量

3.1.1 终端安全管理系统问题排查——TCPView 使用实验

【实验目的】

掌握 TCPView 的使用方法。

【知识点】

TCPView,端口。

【场景描述】

A 公司的安全运维工程师小王怀疑内网终端可能中了木马,需要使用 TCPView 分 析当前终端的网络连接情况,对异常流量进行分析,以便排查分析木马行为。请协助小王 使用 TCPView 工具分析网络流量。

【实验原理】

木马程序运行后,通常会尝试连接远控端,与远控端进行通信,在此过程中通常会打 开某个端口,如果有通信过程就有可能会创建通信进程。TCPView 是 Sysinternals 工具 包中的一款免费软件,该软件是绿色软件不需要安装,直接运行即可。TCPView 主要用 于查看端口和线程,TCPView 虽然是静态显示端口和线程,但由于运行快捷、方便,占用 资源比较少,在排查时可作为监视工具进行辅助分析。

【实验设备】

主机设备: Windows Server 2008 R2 主机 1 台, Windows 7 主机 1 台。 网络设备: 交换机 1 台。

【实验拓扑】

实验拓扑如图 3-1 所示。



图 3-1 终端安全管理系统 TCPView 使用实验拓扑

【实验思路】

使用 TCPView 查看当前网络连接信息。

【实验步骤】

(1) 进入实验对应拓扑,登录右侧 PC 终端,如图 3-2 所示。



图 3-2 登录 PC 终端

(2) 使用账户 Administrator 和密码 123456 登录终端,运行桌面上的 TCPView 程 序,如图 3-3 所示。



图 3-3 TCPView 程序图标

【实验预期】

使用 TCPView 查看网络连接信息。

【实验结果】

(1) TCPView 运行之后主界面如图 3-4 所示。

Street - Sy	sinternals: www.	sysinternals.com						×
File Options	Process View	Help						-
								_
∎[A → ⊡								
Process /	PID	Protoco1	Local Address	Local Port	Remote Address	Remote Port	State	•
13 360EntCli	3892	TCP	win7-PC	818	win7-PC	0	LISTENING	- H
0: 360EntCli	1100	TCP	win7-pc	49178	win-o562vcgrgae	http	CLOSE WAIT	
10: 360EntCli	1100	TCP	win7-pc	49275	win-o562vcgrgae	http	ESTABLISHED	
0: 360EntCli	1100	UDP	win7-PC	50894	*	*		
360EntCli	1100	UDP	win7-PC	50895	*	*		
🖬 [System P	0	TCP	win7-pc	49180	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49181	win-o562vcqrqae	http	TIME_WAIT	=
📰 [System P	0	TCP	win7-pc	49182	win-o562vcqrqae	http	TIME_WAIT	- 11
📰 [System P	0	TCP	win7-pc	49183	win=o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49184	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49185	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49186	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49187	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49188	win=o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49189	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49190	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49191	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49192	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49193	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49194	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49195	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49196	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49197	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49198	win=o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49199	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49200	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49201	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49202	win-o562vcqrqae	http	TIME_WAIT	
🖭 [System P	0	TCP	win7-pc	49203	win-o562vcqrqae	http	TIME_WAIT	
📰 _System P	0	TCP	win7-pc	49204	win-o562vcqrqae	http	TIME_WAIT	
📰 _System P	0	TCP	win7-pc	49205	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49206	win-o562vcqrqae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49207	win-o562vcoroae	http	TIME_WAIT	
📰 [System P	0	TCP	win7-pc	49208	win-o562vcqrqae	http	TIME_WAIT	
🖬 System P	0	TCP	win7-pc	49209	win-o562vcqrqae	http	TIME_WAIT	
System P	0	TCP	win7-pc	49210	win-o562vcqrqae	http	TIME_WAIT	
📰 LSystem P	0	TCP	win7-pc	49211	win-o562vcqrqae	http	TIME_WAIT	
E LSystem P	0	TCP	win7-pc	49212	win-o562vcqrqae	http	TIME_WAIT	
System P	0	TCP	win7-pc	49213	win-o562vcqrqae	http	TIME_WAIT	
LSystem P	0	TCP	win7-pc	49214	win-o562vcqrqae	http	TIME_WAIT	
M LSystem P	0	TCP	win7-pc	49215	win-o562vcqrqae	http	TIME_WAIT	
LSystem P	0	TCP	win7-pc	49216	win-o362vcqrqae	http	TIME_WAIT	
LSystem P	0	TCP	win7-pc	49217	win-0362vcqrqae	http	TIME_WAIT	-
■ LSystem P	0	TCP	win7-pc	49218	win=o562vcqrqae	http	TIME WAIT	
•	_	m	_	_				•
Endpoints: 133	Established: 1	Listening: 22	Time Wait: 93	Close Wait: 1				đ

图 3-4 TCPView运行界面

(2) 单击上方菜单栏中的 View 可以看到两个选项: Update Speed(更新速度)和 Refresh Now(立即刷新)。单击 Refresh Now 命令可以立即刷新当前的进程和网络状态,单击 Update Speed 命令可以选择自动刷新的间隔时间,可以选择 1 秒、2 秒、5 秒和 "暂停刷新",本实验选择刷新间隔为 5 秒,如图 3-5 所示。

🗟 TCPView - Sysinternals: www.sysinternals.com											
File Options Proce	ess View Help										
🖬 A → 🕼	Update Speed	•		1 second		Γ					
Process / PID	Refresh Now	F5		2 seconds		5					
360EntCli 3892	TCP	win7-	<	5 seconds		37					
360EntCli 1100	TCP	win7-	- í	Deveed	Caraca	h -1					
© 360EntCli 1100	TCP	win7-		Paused	space	h=(
0 360EntCli 1100	UDP	win7-P	6	20834	*						
99 360En+C11 1100	IDP	win7-P	<u>^</u>	50895	*						

图 3-5 刷新参数设置

(3) 主内容显示区域显示的内容主要分为12列,分别是 Process(进程名称)、PID(进

程 ID)、Protocol(协议)、Local Address(本地地址)、Local Port(本地端口)、Remote Address(远程地址)、Remote Port(远程端口)、State(连接状态)、Sent Packets(发送的数据包数量)、Sent Bytes(发送了多少字节数据)、Rcvd Packets(接收数据包数量)、Rcvd Bytes(接收了多少字节数据),如图 3-6 所示。

- 6 - F - 1	ile O	fiew - Sys ptions → 🕄	sinternals: ww Process Vie	w.sysinternals.cor w Help	n								
P	rocess	/	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rovd Packets	Rovd Bytes
0	360Er	stCli			win7-PC	818	win7-PC		LISTENING				
R	360Er	atCli	1100	UDP	win7-PC	50894	*	*					
11:0	360Er	atCli	1100	UDP	win7-PC	50895	*	*					
12	Syst	tem P	0	TCP	win7-pc	51241	win-o562vcgrgae	http	TIME WAIT				
	Syst	tem P	0	TCP	win7-pc	51242	win-o562voorgae	http	TIME WAIT				
×.	Syst	tem P	0	TCP	win7-pc	51243	win-o562vcgrgae	http	TIME_WAIT				
E E	Syst	tem P	0	TCP	win7-pc	51244	win-o562vcgrgae	http	TIME WAIT				
E F	Syst	tem P	0	TCP	win7-pc	51245	win-o562vcgrgae	http	TIME WAIT				
	Syst	tem P	0	TCP	win7-pc	51246	win-o562vogrgae	http	TIME WAIT				
1.00	Covet	P P	0	TCP	#in7700	51247	#10-0562vcorose	http	TIME WATT				

图 3-6 主内容显示列

(4) TCPView 默认会把 Remote Address(远程地址)和 Local Address(本地地址)显示为相对应的主机的名称,如果想要设置为显示 IP 地址,单击上方的 Options 菜单,取消 勾选 Resolve Addresses 即可,如图 3-7 所示。

A TCPView - Sysinternals: www.sysinternals.com										
File	Opt	ions Process View Help								
	\checkmark	Show Unconnected Endpoints	Ctrl+U							
Proc	\checkmark	Resolve Addresses	Ctrl+R							
36		Always On Top								
		Font								

图 3-7 Resolve Addresses 选项

(5)刷新时某个进程颜色为绿色时,表示该进程为相对于上次刷新时新增的进程,如图 3-8 所示。

TCPView - Sy	sinternals: www.s	sysinternals.com									- • ×
File Options	Process View	Help									
Process /	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rovd Packets	Rovd Bytes
(i) 360EntCli	3892	TCP	win7-PC	818	win7-PC	0	LISTENING				
360EntCli	1100	UDP	win7-PC	50894	*	*					
③ 360EntCli	1100	UDP	win7-PC	50895	*	*					
System P	0	TCP	win7~pc	51303	win=o562vcqrqae	http	TIME_WAIT				
El System P	0	TCP	win7~pc	51304	win-o562vcqrqae	http	TIME_WAIT				
System P	0	TCP	win7~pc	51305	win-o562vcqrqae	http	TIME_WAIT				
E LSystem P	0	TCP	win7-pc	51306	win-o562vcqrqae	http	TIME_WAIT				
System P	0	TCP	win7-pc	51307	win-o562vcqrqae	http	TIME_WAIT				
E LSystem P	0	TCP	win7-pc	51306	win-o562vcqrqae	http	TIRE_WAIT				
an Loystem P		TUP	win7-pc	51309	win-obervegrgae	nttp	TIME_WAIT				
E Laysten P		TCP	win/~pc	51310	win-obe2vcqrqae	http	TIME_WAIT				
El System P	ě.	100	win7 pc	51312	win-obervegroue	http	TIME WATT				
E Cysten P	ŏ	100	win7mo	81212	winto 552 year and	http	TIME WATT				
El Systam P	ő	TCP	win7-nc	51314	win=o562vcorose	http	TIME WATT				
E System P.	ő	TCP	win7-pc	51315	win-o562veereae	http	TIME WAIT				-
- System P	0	TCP	win7~pc	51316	win-o562vcorose	http	TIME WAIT				
1sass.eze	520	TCP	win7-PC	49160	win7-PC	0	LISTENING				
1 1sass. exe	520	TCPV6	win7-pc	49160	win7-pc	0	LISTENING				
services, exe	508	TCP	win7-PC	49158	win7-PC	0	LISTENING				
services. eze	508	TCPV6	win7-pc	49158	win7-pc	0	LISTENING				
svchost. exe	700	TCP	win7-PC	epmap	win7-PC	0	LISTENING				
svchost.eze	1220	TCP	win7-PC	ms-wbt-server	win7=PC	0	LISTENING				
svchost.exe	752	TCP	win7-PC	49153	win7-PC	0	LISTENING				
svchost.eze	936	TCP	win7-PC	49155	win7-PC	0	LISTENING				
svchost.exe	304	TCP	win7-PC	49159	win7-PC	0	LISTENING				
svchost.eze	1024	UDP	win7-PC	ntp	*	*					
svchost. exe	936	UDP	win7-PC	isakmp		•					
svchost.exe	1536	UDP	win7=PC	sadp							
svchost. exe	1536	UDP	win7-pc	ssdp		:					
svchost. exe	1536	UDP	win7=PC	ws-discovery	:	:					
svchost. exe	1536	UDP	Win/~PC	ws-discovery	:	:					
avenost.eze	1220	100	win7-PC	lpsec-dift		:					
avendet. ere	1836	100	min7=BC	52770							·
avchost ere	1536	TIDP	win7me	62438							
sychost ere	1536	UDP	win7-PC	62439							
avchost ere	700	TCPV6	win7-nc	ecman	win7-ne	0	LISTENING				
sychost, eze	1220	TCPV6	win7-pc	ms-wbt-server	win7-pc	õ	LISTENING				
avchost. exe	752	TCPV6	win7-pc	49153	win7-pc	0	LISTENING				
sychost. exe	936	TCPV6	win7-pc	49155	win7-pc	0	LISTENING				
svchost. eze	304	TCPV6	win7-pc	49159	win7-pc	0	LISTENING				
svchost, exe	1024	UDPV6	win7-pc	123							
svchost.eze	936	UDPV6	win7-pc	500	*	*					•
•											
Endpoints: 62	Established: 0	Listening: 22	Time Wait: 14	Close Wait: 0							

图 3-8 新增的进程信息

(6)当进程颜色为红色时,表示该进程相对于上次刷新时已经销毁的进程,如图 3-9 所示。

TCPview - Sysinternals: www.sysinternals.com											- • ×
File Option	s Process	View Help									
Process /	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rovd Packets	Rovd Bytes
28 360EntCli.	3892	TCP	win7-PC	818	win7-PC	0	LISTENING				
360EntCli.	1100	UDP	win7-PC	50894	*	*					
360EntCli.	1100	UDP	win7-PC	50895		*					
System P.	0	TCP	win7-pc	51317	win-o562vcqrqae	http	TIME_WAIT				
System P.	0	TCP	win7-pc	51318	win-o562vcgrgae	http	TIME_WAIT				
System P.	0	TCP	win7-pc	51319	win-o562vcqrqae	http	TIME_WAIT				
System P.	0	TCP	win7-pc	51320	win=o562vcgrgae	http	TIME_WAIT				
System P.	0	TCP	win7-pc	51321	win-o562vcqrqae	http	TIME_WAIT				
System P.	0	TCP	win7~pc	51322	win-o562vcqrqae	http	TIME_WAIT				
System P.	0	TCP	win7-pc	51323	win-o562vcgrgae	http	TIME_WAIT				
📰 [System P.	0	TCP	win7-pc	51324	win-o562vcqrqae	http	TIME_WAIT				
📰 [System P.	0	TCP	win7-pc	51325	win-o562vcqrqae	http	TIME_WAIT				
📰 [System P.	0	TCP	win7-pc	51326	win=o562vcqrqae	http	TIME_WAIT				
System P.	0	TCP	win7-pc	51327	win=o562vcgrgae	http	TIME_WAIT				
The formation R		200	-1-8								

图 3-9 销毁的进程信息

(7)单击选中要操作的进程,右击会弹出可对该进程进行相应的操作选项,如图 3-10 所示。

CPView - Sy	sinternals: www	.sysinternals.com									
File Options	Process View	Help									
D •											
Process /	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rovd Packets	Rovd Bytes
(3) 360EntCli	3892	TCP	win7-PC	818	win7-PC	0	LISTENING				
360EntCli	1100			50894	*	*					
138 360EntCli	1100 P	rocess Properties		50895	*	*					
a Loysten P	о С	nd Process		51401	Win-obervegrgae	nttp	TINE_WAIT				
E Custem P		ING FTOCODO		51402	win-obervegrgae	http	TIME WATT				
W Sustan P	č i			51403	minness?	http	TIME WATT				
E System P	č C	lose Connection		51405	win-obertogram	http	TIME WATT				
El System P		the sta	0-1-14	51405	winzelf2veeree	http	TIME WATT				
El Systam P	ě V	vnois	Ctri+W	51407	win=o562vcorosa	httn	TIME WATT				
El Systam P	i c	onv	Ctrl+C	51408	#18-6552vectore	http	TIME WATT				
# System P.	č l	ору	Curre	51409	win=o562vcorose	http	TIME WAIT				
System P	ō	TCP	win7-ne	51410	win-off2veeress	http	TIME WAIT				
F System P	ō	TCP	win7-pc	51411	win-o562vcorose	http	TIME WAIT				
#1 [System P	0	TCP	win7-pc	51412	win-o562vcqrqae	http	TIME_WAIT				
#1 [System P	0	TCP	win7-pc	51413	win-o562vcgrgae	http	TIME WAIT				
1sass.exe	520	TCP	win7-PC	49160	win7=PC	0	LISTENING				
1 Isass. exe	520	TCPV6	win7-pc	49160	win7-pc	0	LISTENING				
services.exe	508	TCP	win7-PC	49158	win7-PC	0	LISTENING				
services.eze	508	TCPV6	win7-pc	49158	win7-pc	0	LISTENING				
svchost.exe	700	TCP	win7-PC	epmap	win7-PC	0	LISTENING				
svchost.exe	1220	TCP	win7-PC	ms-wbt-server	win7-PC	0	LISTENING				
svchost.exe	752	TCP	win7-PC	49153	win7-PC	0	LISTENING				
svchost.exe	936	TCP	win7-PC	49155	win7-PC	0	LISTENING				
svchost.exe	304	TCP	win7-PC	49159	win7-PC	0	LISTENING				
svchost.exe	1024	UDP	win7-PC	ntp	•	•					
svohost. eze	936	UDP	win7-PC	isakmp	•						
svchost.exe	1536	UDP	win7=PC	qbaa	•						
svohost. eze	1536	UDP	win7-pc	ssdp							
svohost. ere	1536	UDP	win7"PC	ws~discovery	:	:					
svonost. ere	1036	UDP	#18/"PC	ws-discovery	:	:					
avendet. ere	230	UUT IIII	#101 PL	ipsec dirt	:	:					
svendst. ere	1836	100	#107-DC	82770							
svendst. ere	1834	100	win77mg	40400							
sychost ere	1536	100	win7-00	62439							
sychost ere	700	TCPV6	win7-ne	ecman	win7-ne	0	LISTENING				
sychost ere	1220	TCPV6	win7-ne	ns-mbt-server	win7-ne	ő	LISTENING				
sychost.eze	752	TCPV6	win7-pc	49153	win7-pc	õ	LISTENING				
sychost.eze	936	TCPV6	win7-pc	49155	win7-pc	0	LISTENING				
svchost. eze	304	TCPV6	win7-pc	49159	win7-pc	0	LISTENING				
sychost.eze	1024	UDPV6	win7-pc	123							
svchost, eze	936	UDPV6	win7-pc	500							
svohost. eze	1536	UDPV6	[0:0:0:0:0:0:0:	. 1900	*	*					
4					III						_
Endpoints: 61	Established: 0	Listening: 22	Time Wait: 13	Close Wait 0							
composites or	Consolation of	saturally: 22	Time Wale 15	close trait o							

图 3-10 对选中进程进行操作

(8)选择弹出菜单中的 Process Properties(进程属性),可以查看该进程的名称、版本 以及 Path(路径),单击 End Process 按钮可以结束该进程,如图 3-11 所示。

roperties	s for EntClient.exe: 1100	-2
Version: Path:	客户端组件 互联网安全中心 6.00.0000.2068	
C:\Progra	m Files\Safe\EntClient.exe	
		End Process

图 3-11 进程属性

(9)如果选择弹出菜单中的 Copy 命令,可以将此进程的信息以文本方式复制到系统的剪贴板里,用于记录或其他用途,如图 3-12 所示。

🖧 TCPView - Sy	sinternals	www.sysinternals.com		
File Options	Process	View Help		
🖬 A 🛶 🗊				
Process	PID	Protocol	Local Address	Local Por
() EntCli	1100	UDP	win7-PC	50894
 EntCli svchost.exe svchost.exe svchost.exe svchost.exe svchost.exe svchost.exe svchost.exe svchost.exe svchost.exe 	1100 1024 936 1536 1536 1536 1536 936 1220	Process Properties End Process Close Connection Whois	Ctrl+W	50895 ntp isakmp ssdp ws-discov ws-discov ipsec-msf 11mmr
svchost.exe	1536	Сору	Ctrl+C	53778
svchost. exe svchost. exe svchost. exe svchost. exe svchost. exe	1536 1024 936 1536	UDP UDPV6 UDPV6 UDPV6 UDPV6	win7-PC win7-pc win7-pc [0:0:0:0:0:0:0:	62439 62439 123 500 . 1900
svchost, exe	1536	UDPV6	[fe80:0:0:0:d	. 1900

图 3-12 复制进程信息

(10)单击左上角的"保存"按钮或者按 Ctrl+S 组合键可以保存系统当前运行所有进程的状态信息,如图 3-13 所示。

CPView - Sysinternals: www.sysinternals.com											
File Options	Process View	Help									
🖬 A 🚽 🕅											
Process	PID	Protoco1	Local Address	L							
C EntCli	1100	UDP	win7-PC	50							
EntCli	1100	UDP	win7-PC	50							
svchost.exe	1024	UDP	win7-PC	nt							
svchost.exe	936	UDP	win7-PC	is							
svchost.exe	1536	UDP	win7-PC	55							
svchost. exe	1536	UDP	win7-pc	55							
svchost. exe	1536	UDP	win7-PC	ws							

图 3-13 保存系统当前运行进程状态

(11)保存文件格式为 txt 文本格式,双击打开保存的文本文件,可以看到记录的进程 信息,如图 3-14 所示。

_ Process - 记事本	2											
文件(F) 编辑(E)	格式(O)	查看(V) 帮助(F	H)									
EntClient.exe		1100	UDP	win7-P0	C 50894	*	*					*
EntClient.exe		1100	UDP	win7-P0	50895	*	*					
svchost.exe	1024	UDP	win7-PC	ntp	*	*						
svchost.exe	936	UDP	win7-PC	isakmp	*	*						
svchost.exe	1536	UDP	win7-PC	ssdp	*	*						
svchost.exe	1536	UDP	win7-pc	ssdp	*	*						
svchost.exe	1536	UDP	win7-PC	ws-dis	covery	*	*					
svchost.exe	1536	UDP	win7-PC	ws-dis	covery	*	*					
svchost.exe	936	UDP	win7-PC	ipsec-	nsft	*	*					E
svchost.exe	1220	UDP	win7-PC	11mnr	*	*				1	42	
svchost.exe	1536	UDP	win7-PC	53778	*	*						
svchost.exe	1536	UDP	win7-pc	62438	*	*						
svchost.exe	1536	UDP	win7-PC	62439	*	*						
svchost.exe	1024	UDPV6	win7-pc	123	*	*						
svchost.exe	936	UDPV6	win7-pc	500	*	*						
svchost.exe	1536	UDPV6	[0:0:0:	0:0:0:0	:1]	1900	*	*				
svchost.exe	1536	UDPV6	[fe80:0	:0:0:db	f:609b:e	O6b:celc]	1900	*	*			
svchost.exe	1536	UDPV6	win7-pc	3702	*	*						
svchost.exe	1536	UDPV6	win7-pc	3702	*	*						
svchost.exe	936	UDPV6	win7-pc	4500	*	*						
svchost.exe	1220	UDPV6	win7-pc	5355	*	*						
svchost.exe	1536	UDPV6	win7-pc	53779	*	*						
svchost.exe	1536	UDPV6	[fe80:0	:0:0:db	f:609b:e	O6b:celc]	62436	*	*			
svchost.exe	1536	UDPV6	L0:0:0:	0:0:0:0	:1]	62437	*	*				
System 4	UDP	win7-pc	netbios	-ns	*	*		27	1,350	612	30,600	
System 4	UDP	win7-pc	netbios	-dgm	*	*		4	818	6	1,220	
svchost.exe	752	UDPV6	Lie80:0	:0:0:db	t:609b:e	Ubb:celc]	546	*	*			
360EntClient.e	xe	3892	TCP	win7-P0	818	win7-PC	0	LISTENI	NG			
lsass.exe	520	TCP	win7-PC	49160	win?-P	CÓ	LISTENI	NG				
isass.exe	520	ICPV6	winf-pc	49160	win?-p	c v	LISTENI	NG				
services.exe	508	ICP	win7-PC	49158	win?-P	C U	LISTENI	NG				
services.exe	508	ICPV6	win7-pc	49158	win7-p	c U	LISTENI	NG				-
•	_		_	_	_	_	_	m	_	_		•

图 3-14 保存的进程信息

(12) TCPView 可以按照使用者关注的类型进行排序。例如,按照 State 的状态进行 排序,单击 State 一列即可按照该列状态重新进行排序,如图 3-15 所示。

CPView - Sysinternals: www.sysinternals.com											
File Options	Process View	Help									
								_			
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State V	Sent Packets	Sent Bytes	Rovd Packets	Rovd Bytes
F [System P	0	TCP	win7-pc	51504	win-o562vcqrqae	http	TIME_WAIT				
System P	0	TCP	win7-pc	51505	win-o562vcqrqae	http	TIME_WAIT				
System P	0	TCP	win7-pc	51506	win-o562vcqrqae	http	TIME_WAIT				
System P	0	TCP	win7-pc	51507	win-o562vcqrqae	http	TIME_WAIT				
ESystem P	0	TCP	win7-pc	51508	win-ob62vcqrqae	http	TIME_WAIT				
System P	0	TCP	win7-pc	51509	win-o362vcqrqae	http	TIME_WAIT				
ISystem P	0	TCP	win/~pc	51510	win-ob62vcqrqae	http	TINE_WAIT				
System P	0	TCP	win/~pc	51511	win=ob62vcqrqae	nttp	TINE_WAIT				
ISystem P	0	TCP	win7-pc	51512	win=0362vcqrqae	http	TIME_WAIT				
I Laysten P	0	TCP	win/-pc	51513	win-ob62vcqrqae	http	1106_WA11				
I Loystem P	0	TCP	win/~pc	51519	win-0362vcqrqae	http	TIME_WAIT				
W Loystem P		TCP	win/ pc	51515	win-0562vcqrqae	http	TIME WATT				
WT Creater P	°	TCP	win/-pc	51516	win-0362vcqrqae	http	TIME_WAIT				
09 260En+C14	2002	TCP	min7=PC	010	win courrequide	0	I TOTENTNO				
1 lease ave	520	TCP	win7-PC	49160	win7=PC	õ	LISTENING				=
in irarr ave	520	TOPUS	win7-no	49160	win7-no	õ	LISTENING				
sarvicas ave	508	TCP	win7=BC	49158	win7=BC	õ	LISTENING				
services ere	508	TCPV6	win7-ne	49158	win7-nc	ő	LISTENING				
sychost ave	700	TCP	win7-PC	enmen	win7-PC	õ	LISTENING				
sychost.exe	1220	TCP	win7-PC	ms-wbt-server	win7-PC	õ	LISTENING				
sychost.exe	752	TCP	win7-PC	49153	win7-PC	õ	LISTENING				
sychost ere	936	TCP	win7=PC	49155	win7-PC	ō	LISTENING				
sychost.exe	304	TCP	win7-PC	49159	win7-PC	ō	LISTENING				
sychost, exe	700	TCPV6	win7-pc	eomap	win7-pc	ō	LISTENING				
sychost, exe	1220	TCPV6	win7-pc	ms-wbt-server	win7-pc	0	LISTENING				
sychost, exe	752	TCPV6	win7-pc	49153	win7-pc	0	LISTENING				
svchost.exe	936	TCPV6	win7-pc	49155	win7-pc	0	LISTENING				
svchost.exe	304	TCPV6	win7-pc	49159	win7-pc	0	LISTENING				
System	4	TCP	win7-pc	netbios-ssn	win7-PC	0	LISTENING				
System	4	TCP	win7-PC	microsoft-ds	win7-PC	0	LISTENING				
System	4	TCP	win7-PC	wad	win7-PC	0	LISTENING				
System	4	TCPV6	win7-pc	microsoft-ds	win7-pc	0	LISTENING				
System	4	TCPV6	win7-pc	wsd	win7-pc	0	LISTENING				
wininit.exe	412	TCP	win7-PC	49152	win7-PC	0	LISTENING				
wininit.exe	412	TCPV6	win7-pc	49152	win7-pc	0	LISTENING				
()) EntCli	1100	UDP	win7-PC	50894	*	*					
EntCli	1100	UDP	win7-PC	50895							
svcnost.exe	1024	UDP	win/~PC	ntp							
svcnost.exe	936	UDP	win7=PC	1sakmp	:	*					
svcnost. exe	1330	UDP	win/-FC	ssap	:						
svcnost. exe	1000	100	win/~pc	aadp							
svcnost. exe	1000	UDP	wing PG	ws-ulscovery	:	:					-
4	1000	UDP	win/-PC	ws-discovery	-	•					
				-							
Endpoints: 62	Established: 0	Listening: 22	Time Wait: 14	Close Wait: 0							.4

图 3-15 按 State 状态排序

(13)使用 TCPView 可以查看当前终端中运行的进程、端口、协议、状态、收发数据包数量等状态信息,并可以对某个进程复制状态信息,同时可以导出当前运行时的进程运行状态保存为文本文件,以便后续查看,满足实验预期。

【实验思考】

(1) 使用 TCPView 如何发现流量异常的进程?

(2) 在 TCPView 中,进程的状态都有哪几种? 分别代表什么含义?

3.1.2 Wireshark 网络流量分析实验

【实验目的】

掌握 Wireshark 常用过滤命令的使用。

【知识点】

IP 过滤,端口过滤,HTTP 模式过滤。

【场景描述】

A 公司安全运维工程师小王在日常巡检中发现某台终端流量异常,为获知该终端异常流量的关联信息,小王需要使用 Wireshark 抓取该终端的通信流量进行分析,请协助小王使用 Wireshark 对该终端的通信流量进行分析。

【实验原理】

Wireshark 是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包, 并尽可能显示出最为详细的网络封包资料。Wireshark 使用 WinPcap 作为接口,直接与 网卡进行数据报文交换。

【实验设备】

主机设备: Windows Server 2003 主机 1 台, Windows 7 主机 1 台。 网络设备: 交换机 1 台。

【实验拓扑】

实验拓扑如图 3-16 所示。



图 3-16 Wireshark 网络流量分析实验拓扑

【实验思路】

- (1) 访问 FTP 服务器。
- (2) 访问 Eshop 商城。
- (3) Wireshark IP 筛选数据包。
- (4) Wireshark 端口筛选数据包。
- (5) Wireshark HTTP 模式筛选数据包。

【实验步骤】

1. 访问 FTP 服务器

(1) 进入实验对应拓扑,登录 Windows 7 终端,如图 3-17 所示。



图 3-17 登录 Windows 7 终端

(2)运行浏览器,在地址栏中输入"ftp://172.16.8.72",访问该地址,可见访问 FTP 服务器正常,如图 3-18 所示。

	Image: 10 ftp://172.1	.6.8.72/ 的素引 🗙 🕂						×
(_) → ሮ ŵ	(i) ftp://172.16.8.72		💟	☆	111	•	≡
								-
	ftp://17	2.16.8.72/ 的索引						=
	1 回到上	—层文件夹						
	(all)		 .	Ma 1/20-1	Han .			
	るが		入小	修成的	[[1]]			
	文件:	apachetomcat7setup_veryhuo.com.zip	9000 KB	2018/4/10	15:54:00			_
	文件:	AUTOEXEC.BAT		2015/12/17	0:00:00			
	文件:	CONFIG.SYS		2015/12/17	0:00:00			
	Do	cuments and Settings		2015/12/17	0:00:00			
	文件:	eula.2052.txt	4 KB	2008/1/5	0:00:00			
	文件:	fmw_12.2.1.3.0_wls.jar	819540 KB	2017/8/22	0:00:00			
	ftp			2018/8/27	14:03:00			
	文件:	globdata.ini	2 KB	2008/1/5	0:00:00			
	138	6		2018/4/10	19:11:00			
	文件:	I3861.zip	533737 KB	2017/8/8	0:00:00			
	I. I.	th		2018/4/10	10.22.00			-

图 3-18 FTP 服务器目录

2. 访问 Eshop 商城

在浏览器中新建新标签页,在地址栏中输入"http://172.24.8.36",访问该地址,可见 网站显示正常,如图 3-19 所示。

	Ň	ftp://	172.16.8.72/ 的素引	×	网	奇.NET商城系	统v5.5P	ower By 🗙									×
€	\rightarrow	G	ŵ	i	% 1	72.16.8.72						5	7 ☆		111	1	≡
		۶			搜索	高级搜索		会员:	密码	3:	验证:	8 7 37	登录	注册 忘记:	谿码		
		网奇	ESHOP商旅购。) E	4 55	•											
		www	v.wqeshop.	сo	m						设	为首页	牧藏夹	购物车 简 鬗	英		
	1	ř	「城首页 商品会	计类	精	品推荐	最新商品	3 打折	育品 热销	商品 报价	·中心 新闻中/	i> ∣ ₹	9助中小	↓ 留言薄			
•••	Ы				1 115											1	
•••	Ľ	-	品牌数码 品牌家	电日	尚美能	目早春新装	伴娘礼服	3 热销韩装	春夏手袋 情	目饰品 美肤新品	品 眼部护理 祛斑	訪晒丨保	健饮茶	过季秋装		1	
•••		. • F	51城动态			ži						商品	6分类 ♭			1	
	L	* 网语	FEshop 5.5版隆重出炉		奋	品展示		1 2	3 4	5 6	7 8	Prido	8	波女装			
	L	+ 网合	iEshop 5.5版隆重出炉		1+5	ни не 🥠							早春新新	麦 伴娘礼服		1	
	L	* MR * 제품	FEshop 5.5版隆重出炉								: 3		热销韩	麦 时尚冬靴			
		+ 网营	FEshop 5.5版隆重出炉										#	洋美包			
		+ 网营	FEshop 5.5版隆重出炉										OL新资源	む 春夏手袋		1	
		+ 网络	FEshop 5.5版隆重出炉										情侣饰品	品 GUESS新款	b		

图 3-19 访问网站

【实验预期】

- (1) Wireshark 查看指定 IP。
- (2) Wireshark 查看指定端口。
- (3) Wireshark 查看指定 HTTP 数据包。

【实验结果】

1. Wireshark 查看指定 IP

(1) 在终端桌面上,双击 Wireshark 图标快捷方式,运行 Wireshark 程序,如图 3-20 所示。

(2) 在程序首页中,单击"本地连接"链接开始监听该网卡,如 图 3-21 所示。由于本实验终端中只有一块网卡,因此仅能监听该 网卡。如实际终端有多块网卡,请选择对应网卡进行监听。



(3) 在表达式栏中输入表达式"ip.src==172.16.8.36",表明 图 3-20 运行 Wireshark 查找源 IP 地址为 172.16.8.36 的数据包,单击"箭头"按钮查询源 程序

IP 数据包,可以筛选出相关的数据包记录。如果没有流量记录筛选出来,可重新刷新浏 览器访问网站的页面,以便产生数据流量,如图 3-22 所示。

▲ Wireshark 网络分析器			- • ×
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 7	无线(W) 工	具(T) 帮助(H)	
	. 匪		
Apply a display filter … 《Ctrl-/>			▶ 表达式… +
欢迎使用 Wireshark 捕获 …使用这个过速器: □ Knter a capture filter … 本地连接		l interfaces show	a *
学习			
用户指导 Wiki 问题与解答 邮件列表			
正在运行 Wireshark2.6.2 (v2.6.2—O—glb3cedbc).接受自动更新。			
2 已准备好加载或捕获	无分组		Profile: Default

图 3-21 Wireshark 开始页面

▲ *本地	连接																								0	-		×
文件(F)	编辑	(E)	视图(V)	跳转	(G)	捕	夫(C)	分	祈(/	A)	统计	H(S)	E	电话	(Y)	形	戋(W)	I	.具(T)) 帮	勖助(H)					
	6		010	X	G	٩	Þ	•	۶.	Ŷ	₽ [Ð,	Q,	€,	1										
ip. sz	rc== 1'	72.16	8.36																			X		•	表词	±±	•	+
No.	Т	ime			S	ourc	e]	Dest	ina	tion	n				Prot	ocol	Lei	ngth	Inf	0			
	30	.006	748		1	72.	16.	8.36	5			-	172	.1	6.8	.72	2			TCP			54	491	167	÷ 2	1 [FI
	60	.008	064		1	72.	16.	8.30	5			1	172	.1	6.8	.72	2			TCP	•		54	491	167	→ 2	1 [AC
												_		_														b.
				_	_	_			_		_	_	_	-	_	_	_											-
▷ Fran	me 6:	54	byte	25 (on w	ire	: (4	32	bit	s),	54	b	yte	25	cap	tur	red	(43	2 b	its)	on	int	erf	ace	0			A
▷ Ethe	ernet	: II.	, Sr	:: 6	92:7	/b:0	d:4	7:0	9:8	5 (02:	7b	:0d	1:4	7:0	99:8	35)	, Ds	t:	02:c	13:7	2:39):1b	:30	(0	2:d	3:72	
► Tnta	ornot	- Pro	ntori	11	lone	ion	1	Sn	· ·	173	16	: 2	36		Nc+	-• 1	172	16	87	2	_	_	_				Þ	È
6000	02 0	13 7	2 30	1h	30	02	7h	04	17	a	9 80	: 0	8 0	10	15	00			. 0.	5.0	2	. E .						۲
0010	02 0	28 0	1 61	40	00	80	06	00	90	a	10	, 0 1 0	8 2	24	ac	10		.(.a	ດ	1.1		¢						
0020	08 4	18 ci	9 0f	00	15	dc	94	4d	66	fo	61	- 9	0 f	F1	50	10		.н	e 	. M-	F·o·	.́р.						
0030	00 1	Fe 6	B a7	00	00				50					-	- 0			· · h ·										
0 2	wire	shark	4770	74C3-	-DAOC	-452	A-4.	•3_20)180	3271	5091	0_a	0362	24. 1	peap	ng	分组	: 7	·Ε	显示	: 2 ((28.61	0 1	Profi	ile:	Defa	wlt	

图 3-22 筛选源 IP 数据包

(4) 在表达式栏中输入表达式"ip.dst = = 172.16.8.72",表明查找目的 IP 地址为 172.16.8.72 的数据包,单击"箭头"按钮查询目的 IP 数据包。如无流量记录,可刷新浏览 器页面,以便产生数据流量,如图 3-23 所示。

4 *本地	连接																	•	×
文件(F)	编辑(E) 社	见图(V)	跳转((G) 捕藜	尧(C)	分析	(A)	统	+(S)	电话	(Y)	无线(W)]	[具(T)	帮助	助(H)			
		(10) X	G	ې 🗇	•	Ŷ	₽			⊕ 		Q. 🎹							
ip. d	st== 172.16.8	3. 72														\times \rightarrow	💌 表	达式…	+
No.	Time		So	nce					Destir	atio	n			Prote	ocol	Length	Info		
	3 0.006	748	17	2.16.	8.36				172.3	16.8	.72			TCP		54	49167	→ 21	[FI
L	6 0.008	964	17	2.16.	8.36				172.3	16.8	.72			TCP		54	49167	→ 21	[AC
•					m														Þ
▶ Fra	me 3: 54	bytes	on wi	re (4	32 b:	its)	, 5	54 b	ytes	cap	otur	ed (4	432 b	its)	on	interf	ace 0		
▶ Eth	ernet II,	Src:	02:7b	.0d:4	7:09	:85	(02	2:7b	:0d:	47:6	9:8	5), I	Dst:	02:d	3:72	:39:1b	:30 (0	2:d3:	72:3
▷ Int	ernet Pro	tocol	Versi	on 4,	Src	: 17	2.1	6.8	.36,	Dst	:: 1	72.1	6.8.7	2					
⊳ Tra	nsmission	Contr	rol Pr	rotoco	1, S	rc P	ort	:: 4	9167	, D⊴	st P	ort:	21,	Seq:	1,	Ack: 1	, Len:	0	
•						_	_												4
0000	02 d3 72	39 1b	o 30 6	92 7b	0d /	47 6	9 8	35 0	8 00	45	00		r9.0	{ · G		Ε·			
0010	00 28 01	60 40	00 8	30 06	00	00 a	ac 1	LØ 0	8 24	ac	10	· (·`@··		· · · \$				
0020	08 48 c0	0f 00	ð 15 d	lc 94	4d	65 f	Fc 6	5f 9	0 f0	50	11	۰H		· Me	· o · ·	P۰			
0030	00 fe 68	a7 00	00 0										h···						
07	wireshark_	4770F4C3	3-DAOC-	452 A-A -	·3_201	80821	71509	910_a	.03624.	pcap	ng :	分组:	90 ·	已显示	: 2 (2.2%) :	Profile:	Defau	Lt

图 3-23 筛选目的 IP 数据包

2. Wireshark 查看指定端口

(1) 在表达式栏中输入表达式"tcp.port==21",表明查找数据包流经端口为 21 的 TCP 数据包,单击"箭头"按钮查询流经端口 21 的数据包。如无流量记录,可刷新浏览器 访问 FTP 网站页面,以便产生数据流量,如图 3-24 所示。

4本地	连接					
文件(F)	编辑(E) 视图	图(V) 跳转(G) 捕获(C) 分析(A) 统计(S	;) 电话(Y) 无线(V	V) 工具(T) 帮助	(H)
	601	1 🕱 🖸 🤇 🗢 🕫	> 🕾 T 🕹 🗖 🖡			
tep.;	port==21					🛛 🔜 🔹 表达式… 🛛 🕇
No.	Time	Source	Des	tination:	Protocol	Length Info
	3 0.00674	8 172.16.8	.36 17	2.16.8.72	TCP	54 49167 → 21 [FI
	4 0.00799	9 172.16.8	.72 17	2.16.8.36	TCP	60 21 → 49167 [AC
	5 0.00800	8 172.16.8	.72 17	2.16.8.36	TCP	60 21 → 49167 [FI
L	6 0.00806	4 172.16.8	.36 17	2.16.8.72	TCP	54 49167 → 21 [AC
•						•
D Ena	ma 3 · 5/1 hv	tes on wire (13	2 hits) 51 hvt	es cantured (/	132 hits) on i	nterface 0
⊳ Fth	ernet II S	rc · 02 · 7b · 0d · 47	·09·85 (02·7b·0	d·47·09·85) [)st· 02·d3·72·	39·1h·30 (02·d3·72·3
▶ Int	ernet Proto	col Version 4.	Src: 172.16.8.3	6. Dst: 172.16	5.8.72	55110150 (021051721
▶ Tra	nsmission C	ontrol Protocol	, Src Port: 491	.67, Dst Port:	21, Seq: 1, A	ck: 1, Len: 0
				,	, , ,	,
•			III			•
0000	02 d3 72 3	9 1b 30 02 7b	0d 47 09 85 08	00 45 00 ···	•9•0•{ •G•••E	•
0010	00 28 01 6	0 40 00 80 06	00 00 ac 10 08	24 ac 10 ·(·	`@··· ···\$·	
0020	08 48 c0 0	f 00 15 dc 94	4d 65 fc 6f 90	f0 50 11 ·H·	····· Me·o··P	-
0030	00 fe 68 a	7 00 00		· · ł	1 · · ·	
07	Internet Prot	tocol Version 4 (ip),	20 bytes	分组: 17	16 ・ 已显示: 4 (2.	3%) Profile: Default

图 3-24 筛选流经端口 21 的数据包

(2) 在表达式栏中输入表达式"tcp.port==80",表明查找数据包流经端口为80的 TCP数据包,单击"箭头"按钮查询流经端口80的数据包。如无流量记录,可刷新浏览器 访问网站的页面,以便产生数据流量,如图3-25所示。

6	本地	连接																					-		•	×
文	4(F)	编辑	异(E)	利	图()图	V)	跳转	(G)	捕	夫(C)	分	折(A)) \$	充计(S)	电话	(Y)	无线(V	V) I	.具(T)	帮	助(H)				
		<u>a</u> (015	X	G	٩	Ð	•	27	1	1			Ð,	Q, (Q. 🎹								
	tcp. p	ort=	80																			X	•	表达	£	+
No.			Fime				S	ourc	e					De	stin	ation	a			Prot	ocol	Length	Inf	,		•
	4	157	290	.05	183	1	1	.72.	16.	8.36				17	2.1	6.8	.72			HTT	Р	536	GE1	/in	nage	. a
	4	158	290	.05	367	5	1	72.	16.	8.72				17	2.1	6.8	.36			ТСР		1514	1 80	→ 49	9177	[
	4	159	290	.05	368	31	1	72.	16.	8.72	1			17	2.1	6.8	.36			HTT	Р	281	L HTT	P/1.	1 20	96
	4	60	290	.05	371	.6	1	72.	16.	8.36	,			17	2.1	6.8	.72			ТСР		54	491	.77 -	80	[]
	4	162 :	290	.26	847	2	1	.72.	16.	8.72				17	2.1	.6.8	.36			TCP		66	9 [TC	P Du	ıp A(CK
4	_		_	_	_	_	_	_		_	_	_	_		_	_	_									
	-	2	07	~						(50)						_			(520		`	· .	<i>c</i>	0		
	Fran	ie z	97: - T	- 60	o Dy	/tes	s or	1 W3	lre	(528	5 0:	ιτs, - //), (56 E	ογτε	25 0	арт	urea	(528	D10	(S) C	on 1nte	erta	ce Ø		72.7
	Ethe	erne	t 1	1,	Sro		92:J	·D:6	a:4	/:0	1:8:	5 (E	02:	/b:6	0a:4	17:6	19:8	5), U	st: 0	02:a	3:72	2:39:10	0:30	(02	: a3:	/2::
	Inte	erne	τΡ	rot	2000	DT /	/ers	510r	,4 ۱	Sro		L/2.	.16	. 8 . :	56,	UST		/2.16	.8.7	2	0	1		-	-	-
	Iran	15M1	551	.on	Cor	itro	DT F	rot	:000	1, 1	brc	POI	rt:	491	L//,	, Ds	τΡ	ort:	80, 3	Seq:	0,	Len: 0	2			
																							_			•
<u> </u>				_																		-	_			,
00	00	02	d3	72	39	1b	30	02	7b	0d	47	09	85	08	00	45	00	· · r	9.0.	{ · G	i · · · ·	·E·				
00	10	00	34	-01	10	40	00	80	60	00	1-	ac	10	80	24	ac	10	- 4 -	- d@		· · · ¥	5				
00	20	20	48	60	19	00	50	40	†a	0e	10	00	00	00	00	80	02	• H •	···P@							
00	40	20 04	02	00	00	00	00	υZ	04	05	υ4	91	05	05	00	01	01	• • •								
0	2	Int	erne	t Pr	oto	:ol \	/ersi	on 4	l (ip), 20	byt	es					分组	: 481	· 已显	示: 2	248 (5	51.6%)	Profi	le: D	efaul	.t

图 3-25 筛选流经端口 80 的数据包

3. Wireshark 查看指定 HTTP 数据包

(1) 在表达式栏中输入表达式"http.request.method = = "GET"(英文符号)",表明 查找 HTTP 请求包中 GET 方法类型的数据包,单击"箭头"按钮查询 GET 数据包,如 图 3-26 所示。

*本	地连接																					_	-	×	2
文件(F) 编辑(E) 1	观图(\	0	跳转	(G)	捕药	€(C)	分	析(A)) \$	充计(S)	电话	(Y)	无线	戋(W)	I	Į (T)	帮助	b(H)				
			010	X	G	٩	¢	⇒ 9	27	1	Ŀ			Ð,	Q,	Q. 1									
htt	p. request	t. met	hod==	"GET	"																\times	•	表达式…	• •	۲
No.	Ti	me			S	ourc	6					De	stin	ati o	n			1	rotoc	:01	Length	Info			*
	210 28	3.8	7948	2	1	72.	16.8	3.36	5			17	72.1	6.8	3.72	2		ł	HTTP		580	GET	/ HTT	P/1	1
+	323 28	9.5	0807	6	1	72.	16.8	3.36	5			17	72.1	6.8	3.72	2		ł	ITTP		650	GET	/Temp	olat	
	325 28	9.5	1608	8	1	72.	16.8	3.36	5			17	72.1	6.8	3.72	2		ł	HTTP		628	GET	/imag	ges/	
	328 28	9.5	5573	8	1	72.	16.8	3.36	5			17	72.1	6.8	3.72	2		ł	HTTP		671	GET	/Temp	lat	
	330 28	9.5	6299	4	1	72.	16.8	3.36	5			17	72.1	6.8	3.72	2		ł	ITTP		619	GET	/pic/	log	
	222.28	0 5	2222	a	1	72	16 5	2 26	:			17	70 1	6 9	2 72	2			ITTD		634	CET	/iman	ine l	Ŧ
-																									_
	[Strea	m ir	ndex	: 1]																				٠
	[TCP S	egme	ent	Len	: 5	26]																			
	Sequen	ce r	numb	er:	1		(rel	ati	ve	seq	uen	ice	num	ber)										1
	[Next	sequ	ienc	e n	umb	er:	527	1	(r	ela	tiv	re s	equ	enc	e n	numb	er)]								1
	Acknow	ledg	gmen	t n	umb	er:	1	(rel	ati	ve	ack	nu	mbe	r)										Ŧ
٠																								•	
0000	02 d	3 72	39	1b	30	02	7b	0d	47	09	85	08	00	45	00		••r9	·0·{	٠G٠		Ε·			_	*
0010	02 36	5 01	66	40	00	80	06	00	00	ac	10	08	24	ac	10		- 6 - f	@···		· ·\$				0	1
0020	08 48	8 с0	19	00	50	40	fa	0e	1f	74	17	ce	f3	50	18		٠H٠٠	· P@ ·	٠·t		р.				
0030	01 00	0 6a	b5	00	00	47	45	54	20	2f	20	48	54	54	50		٠·j·	· · GE	Т/	HT	TP				
0040	2f 31	1 2e	31	0d	0a	48	6f	73	74	3a	20	31	37	32	2e	/	/1.1	· · Ho	st:	17	2.				Ŧ
0 7	wires	hark_	4770F	4C3-	DACC	-452	A•••20	1808	2715	0910	_a03	3624.	pcap	ng	分组	1: 26	10 ·	已显	示: 1	28 (4	1. 9%)	Profi	le: Defa	ult	

图 3-26 筛选 GET 数据包

(2) 在浏览器中访问 172.16.8.72 网站,在网站首页导航栏中,单击"留言簿"链接,在 "内容"处输入"test",Email 处输入"test@qianxin.com","名字"处输入"test",然后单击 "提交"按钮,以便产生 POST 类型数据包,如图 3-27 所示。

Į.] ftp://	172.16.8.72/ 的素引	×	留言薄 - 网	奇.NET商城系统	w5.5P 🗙	+								×
✐→	e G	۵	i 🔏	172.16.8.	72/Guest.asp:	х				•••	▼ ₹	7	lii\		≡
	P		搜	素高级	叟素	会员:	密码	i :	验证:	8	51 📲	录 注册 忘词	密码		· · · · ·
	网奇	ESHOP商城购	均系统	5.5											
	WW	w.wqeshop	.com							设为首了	□ 收藏共	购物车 简 9	髌│ 英		
	Ā	商城首页 商品	分类	精品推荐	最新商品	打折i	商品 │ 热销ī	商品 报(いましん 新闻	闻中心	帮助中	心 留言薄			
		品牌数码 品牌家	『甩 时尚	美食 早春	所装 伴娘礼服	热销韩装	春夏手袋 情(当饰品 美肤	新品 眼部护埋	祛斑防晒	保健饮3	₭ 过季秋装			
	您的位置	置:商城首页 >> 留言酒	薄												
	0 A	商品分类		● 留言!	節										
	⇒品牌	女装				留言	内容							1	
	今年 라운	■春新装 ≤娘礼服			留言者:田野	200	8-12-15 10:10:20)					~		
	⇒煮	》销韩装 +**夕教				店主	回复:								
	⇒花样	美包		[1]				当前页1	,共1页 当前留言	前为1-1,4	、 1个留言		Go		
		山新姿态 i夏手袋			test										
	⇒¶	皆旧饰品 iUESS新款包		内容:											
	⇒美容	化妆						4							
	->∎	部护理		Email: タシ	test@quanxin.com	* ☑ 隐	蔵邮件地址								
	 ⇒ ⇒ り 	5斑防晒 5敏感		-47-	cube	JEA									
	⇒品牌	数码 星													
	¢∦	 詩基亚													•••••

图 3-27 在网站提交数据

(3) 返回 Wireshark 程序中,在表达式栏中输入表达式"http.request.method = = "POST"(英文符号)",表明查询 HTTP 请求包中 POST 类型数据包,单击"箭头"按钮查询 POST 数据包,如图 3-28 所示。

🙍 *本地	连接																							-		23
文件(F)	编辑(E) 衫	V)图(V	/)	跳转	(G)	捕药	₹(C)	分	折(A)) #	充计(S)	电话	(Y)	无	毵(W) 工	具(T)	帮)助(F	1)				
	6		010	X	G	٩	¢	⇒ 9	2 7	1	2 3			€ 	Q,	Ξ,	壐									
http.	. reques	t. metł	10 d==	"POS	Τ"																×	<	•	表达	त	+
No.	Ti	me			S	ource	9					De	stin	ation	n				Prot	ocol	Le	ngth	Info)		
2	689 98	31.19	355	1	1	72.	16.8	3.36				17	2.1	6.8	.72	2			HTTI	Р		734	POS	T /F	Revi	ew.a
•			_		_								_		_	_										•
▷ Fra	me 26	39: 7	734	byt	es	on	wir	e (5	5872	2 b:	its), 1	734	byt	es	са	ptur	red (587	2 b	its) on	int	terf	ace	0 ^
▷ Eth	ernet	II,	Src	: 0	2:7	b:0	d:4	7:09	9:85	5 (6	92:1	7b:(9d:4	17:0	99:8	85)	, Ds	st: 0)2:d	3:7	2:3	9:1b	:30	(02	:d3:	7:
▷ Int	ernet	Prot	toco	ol V	ers	ion	4,	Sro	:: 1	172	.16	.8.3	36,	Dst	:: 1	172	.16.	8.72	2							
⊳ Tra	nsmis	sion	Con	itro)1 P	rot	осо	1, 9	Src	Por	٠t:	493	192,	Ds	st F	Por	t: 8	30, 5	eq:	20	57,	Ack	: 28	3966	, Le	n:
⊿ Hyp	ertex	t Tra	ansf	er	Pro	toc	ol																			
•							11																			•
0070	0a 5	5 73	65	72	2d	41	67	65	6e	74	3a	20	4d	6f	7a		۰Use	er-Ap	g en	t:	Moz					
0080	69 6	c 6c	61	2f	35	2e	30	20	28	57	69	6e	64	6f	77		illa	a/5.0) (Win	dow					
0090	73 2	ð 4e	54	20	36	2e	31	3b	20	72	76	3a	36	31	2e		s Nī	F 6.1	ι;	rv:	61.					
00a0	30 2	9 20	47	65	63	6b	6f	2f	32	30	31	30	30	31	30		0) (Gecko) /2	010	010					
00b0	31 2	ð 46	69	72	65	66	6f	78	2f	36	31	2e	30	0d	0a		1 F:	irefo) x/	61.	Ø. ·					-
07	HTTP	User-J	Agent	hea	der	(htt	p. use	er_ag	ent)	, 79	byt	es			分	组:	2962	·Ε	显示	: 1	(0.0	%)	Profi	le: I	efaul	t ai

图 3-28 筛选 POST 数据包

(4) Wireshark 可以对当前终端的网络流量进行抓取,并对抓取到的数据包,根据条件进行筛选过滤,获得关注的数据包,并可查看数据包中的数据内容,满足实验预期。

【实验思考】

(1) 如何使用 Wireshark 查看 ICMP 包?

(2) 怎样查看一条相关联的数据流信息?

3.2 操作系统

3.2.1 终端安全管理系统问题排查——Autoruns 使用实验

【实验目的】

掌握终端安全管理系统问题排查工具 Autoruns 的使用方法。

【知识点】

Autoruns。

【场景描述】

A 公司的安全运维工程师小王巡检时怀疑公司某台终端运行有问题,在终端查找问题时,因为系统内置的 msconfig 工具不能完全显示所有自启动项,所以小王使用 Autoruns 工具进行启动项的查看。请协助小王使用 Autoruns 进行检查。

【实验原理】

操作系统的自启动服务或程序是因为某些应用程序正常运行是有前提的,必须在操 作系统引导过程中初始化相关联的服务,应用程序才能正常运行。而某些恶意代码也会 将自身的攻击程序或服务设置在操作系统自启动阶段,以获取系统的某些权限或免疫安 全防护措施。

Autoruns 是 Systemals Suite(故障诊断工具套装)的一部分。它能够显示在 Windows 启动或登录时自动运行的程序,并且允许用户有选择地禁用或删除它们,例如, 那些在"启动"文件夹和注册表相关键中的程序。此外,Autoruns 还可以修改包括 Windows 资源管理器的 Shell 扩展(如右键弹出菜单)、IE 浏览器插件(如工具栏扩展)、 系统服务和设备驱动程序、计划任务等多种不同的自启动程序。

【实验设备】

主机设备: Windows Server 2008 R2 主机 1 台, Windows 7 主机 1 台。 网络设备: 交换机 1 台。

【实验拓扑】

实验拓扑如图 3-29 所示。



图 3-29 Autoruns 使用实验拓扑

172.16.8.36/24 (以实际IP地址为准) 终端PC: 172.16.8.30/24 (以实际IP地址为准)

【实验思路】

使用 Autoruns 查看并管理启动项。

【实验步骤】

(1) 进入实验对应拓扑,使用 Administrator 账户,输入密码 123456,登录右侧的终 端 PC,如图 3-30 所示。



图 3-30 登录终端 PC

(2) 运行桌面上的 Autoruns 图标快捷方式运行程序,推荐以管理员身份运行该程 序,如图 3-31 所示。



图 3-31 运行 Autoruns 程序

【实验预期】

使用 Autoruns 查看自启动项。

【实验结果】

(1) Autoruns 程序运行的主界面默认显示在 Everything 选项卡中,如图 3-32 所示。

-		S	in the second second	1 1925	508	"" all u a lui	the first
Everything	Total Evaluation Statement Fundation	lerer EM Sched Ind Tasks	ISA Providers	Drivers p - Ceders	The Reat Even	to the tensor blinder	1 in Appl
City City Control Cont	explore interfected	Ditte	aug services	. Univers 200 codeca	T dout Execu	ite i ges, inage rijaos	hank Poppa
orun Entry	Description	Publisher	image	ran	Imestamp	virus i	xa
HKLM\SYSTEM\CurrentContr	olSet\Control\SafeBoot\AtemateShell				2009/7/14 12:37		
Crnd.exe	Windows 命令处理程序	Microsoft Corporation	c:\wind	ows\system32\cmd.exe	2010/11/20 17:00		
HKLM\SOFTWARE\Microsoft	Windows (Current Version \Hun			(1) 000 000 () (2018/8/21 10:29		
Safetray	安全防护中心模块		c:\progr	ram files \360\360safe \safem	2018/4/17 0:43		
TINLM (SUP I WARE Microsoft	Modeure Setup Unstalled Components	Manual Compation	- Autor		2011/4/12 15:18		
 Browser Customizations Manage Weadows 	Windows 主进程 (hundi 32)	Memoria Corporation	c. wind	ows system 32 vundi 32.exe	2003/7/14 7:41		
	Windows Mail	Menselt Corporation	c. progr	am nes windows mai winnal.	2009/7/14 7.42		
Themes Setup	Mindows 主应柱 (ndididididididididididididididididididi	Monselt Corporation	c:\wind	ows/system32/recour32.exe	2009/7/14 7:59		
Viodowe Desidoo Llod	Martison(c) 注册服务器	Monselt Corporation	c:\wind	ows/sustem32/mosur32.exe	2003/7/14 7:58		
HKI M\Software\Classes\7\Sh	elEx/ContextMenuHandlers		0.000	owa ayatambe regaribe.exe	2018/8/21 14:05		
V Safe Ext	安全卫士 系统扩展模块		c./orog	ram files\ safe\utils\s	2016/10/20 12:08		
SoftMarExt	教件管家		c:\progr	ram files' safe\softmg	2015/5/27 15:47		
HKLM\Software\Classes\Direct	tory\ShellEx\ContextMenuHandlers				2018/8/21 10:29		
✓ SafeExt	安全卫士 系统扩展模块		c:\progr	ram files_safe\utils\s	2016/10/20 12:08		
HKLM\Software\Classes\Direct	ctory\Background\ShellEx\ContextMer	uHandlers			2018/8/21 14:05		
Gadgets	边栏抱动目标	Microsoft Corporation	c:\progr	ram files/windows sidebar/sb	2009/7/14 9:09		
SoftMgrExt	软件管家		c:\progr	ram files\safe\softmg	2015/5/27 15:47		
HKLM\Software\Classes\Fold	er\ShellEx\ContextMenuHandlers				2018/8/21 10:29		
SafeExt	安全卫士 系统扩展模块		c:\progr	ram files \ safe \utils \s	2016/10/20 12:08		
HKLM\Software\Microsoft\Wi	ndows\CurrentVersion\Explorer\Shellic	onOverlayIdentifiers			2018/8/21 10:29		
I Diel/Guneri lo	o 安全卫士 太马防火债模块		c./oma	ram files\safe\safem	2016/4/15 16:44		
in insection in						the second se	

图 3-32 Autoruns 运行界面

(2)在 Everythings 选项卡中,右击任意一个注册表项,会弹出该项目可操作的内容, 该菜单内容与 Autoruns 菜单栏的 Entry 菜单内容是一致的,如图 3-33 和图 3-34 所示。



图 3-33 Entry 菜单

KnownDLLs 😭 Winlogon 🔍 Wi	insock Providers 🎯 Print Monitors	LSA Providers	ork Providers 🗱 WMI	Sidebar Gadgets	Mi Office
🖾 Everything 🏄 Logon 🗧 Explorer	Internet Explorer Scheduled Ta:	sks 🗱 Services 🥬 Drivers	Ever Codecs Boot Execute	e Image Hijacks	AppInit
Autorun Entry Description	Publisher	Image Path	Timestamp	VirusTotal	
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoo	ot\AtemateShell		2009/7/14 12:37		
	理程序 Microsoft Corporation	c:\windows\system32\cm	d.exe 2010/11/20 17:00		E
HKLM\SOFTWARE\Microsoft\Windows\CurrentVen	sion\Run		2018/8/21 10:29		
☑ Safetray 安全	Delete Ctrl+D	are (Beijing c:\program files\360\360s	afe\safem 2018/4/17 0:43	无法解析服务	5器的名称5
HKLM\SOFTWARE\Microsoft\Active Setup\Int	Delete Cul+D		2011/4/12 15:18		
Image: Browser Customizations Windows 主	Copy Ctrl+C	c:\windows\system32\run	dll32.exe 2009/7/14 7:41		
Microsoft Windows Windows Ma	lump to Entry	c:\program files\windows r	nail\winmai 2009/7/14 7:42		
☑ 🗋 n/a Windows 主	Sump to Endy	c:\windows\system32\run	dll32.exe 2009/7/14 7:41		
Themes Setup Microsoft(C)	Jump to Image	c:\windows\system32\reg	svr32.exe 2009/7/14 7:58	无法解析服务	5器的名称:
Windows Desktop Update Microsoft(C)	Varify Image	c:\windows\system32\reg	svr32.exe 2009/7/14 7:58		
HKLM\Software\Classes*\ShellEx\ContextMer	verny image		2018/8/21 14:05		
✓ SafeExt 安全卫士	Check VirusTotal	c:\program files\ safe\utils	\s 2016/10/20 12:08		
☑ SoftMgrExt 软件管路	Process Explorer	c:\program files\ safe\soft	ng 2015/5/27 15:47		
HKLM\Software\Classes\Directory\ShellEx\Cor	Process Explorer		2018/8/21 10:29		
SafeExt 安全卫士	Search Online Ctrl+M	c:\program files\safe\utils	s 2016/10/20 12:08		
HKLM\Software\Classes\Directory\Background	Find Ctrl+F		2018/8/21 14:05		
✓ Gadgets 边栏拖动目		c:\program files\windows a	sidebar\sb 2009/7/14 9:09		
✓ SoftMgrExt 软件管路	Properties Alt+Enter	c:\program files\ safe\softr	ng 2015/5/27 15:47		
HKLM\Software\Classes\Folder\ShellEx\ContextMe	nuHandlers	-	2018/8/21 10:29		
■ SafeExt 安全卫士系统	统扩展模块	c:\program files\ safe\utils	\s 2016/10/20 12:08		
HKLM\Software\Microsoft\Windows\CurrentVersion	\Explorer\ShellIconOverlayIdentifiers		2018/8/21 10:29		
■ DiskGuard Ico 安全卫士木。	马防火情模块	c:\program files\ safe\safe	m 2016/4/15 16:44		

图 3-34 右击显示菜单

File Entry Options User Help □ □ □ ↓ Hide Empty Locations □ □ ↓ Hide Microsoft Entries ● Knowr ✓ Hide Windows Entries	
Everyth Hide Microsoft Entries Knowr ✓ Hide Windows Entries	
S Known ✓ Hide Windows Entries	et E
	ders
Autorun Entry Hide VirusTotal Clean Entries	
HKCU\Sc Scan Options	
Font	

(3) 在菜单栏的 Options 中提供了内容显示的开关功能,如图 3-35 所示。

图 3-35 Options 菜单

(4) 在 Options 菜单中, Hide Empty Locations 表示隐藏空位, 当注册表的键没有键 值或子键时不显示该注册表路径, 因为键值为空时代表没有数据, 也就没有显示的必要 性, 所以该选项的默认设置是勾选状态, 取消勾选后会显示注册表中键值为空的内容, 如 图 3-36 所示。

Autoruns [WIN]	7-PC\Administrator] - Sysinte	ernals: www.sysinternals.	com					8	- • ×
File Entry Opti	ons User Help								
	K 🎼 Filter:								
KnownDLLs	🚨 Winlogon 🛛 🚳 V	Vinsock Providers	Print Monitors	LSA Providers	Netwo	ork Providers	SH WMI	Sidebar Gadgets	Office
Everything	Logon S Explorer	@ Internet Explorer	關 Scheduled Tasks	Services	Sei Drivers	Eug Codecs	Boot Execute	Image Hijacks	AppInit
Autorun Entry	Description	Publi	sher	Image Pa	th	Time	estamp	VirusTotal	
HKLM\System\0	CurrentControlSet\Control\Terminal	Server\Wds\rdpwd\StartupP	rograms			2010	/11/21 5:35		E
HKLM\SOFTW/	RE\Microsoft\Windows NT\Curren	nt Version \Winlogon \App Setu	p			2018	/8/21 14:04		
HKLM\Software	Policies\Microsoft\Windows\Syste	em\Scripts\Startup							
HKCU\Software	Policies\Microsoft\Windows\Syste	em\Scripts\Logon							
HKLM\Software	Policies\Microsoft\Windows\Syste	em\Scripts\Logon							
HKCU\Environm	ent\UserInitMprLogonScript					2018	/3/7 16:23		
HKLM\Environm	ent\UserInitMprLogonScript								
HKLM\SOFTW/	RE\Microsoft\Windows NT\Curren	ntVersion\Winlogon\Userinit				2018	/8/21 14:04		
HKLM\SOFTW/	RE\Microsoft\Windows NT\Curren	ntVension\Winlogon\VmApple	t in the second s			2018	/8/21 14:04		
HKLM\Software	Policies/Microsoft/Windows/Syste	em\Scripts\Shutdown							
HKCU\Software	Policies/Microsoft/Windows/Syste	em\Scripts\Logoff							
HKLM\Software	Policies/Microsoft/Windows/Syste	em\Scripts\Logoff							
HKCU\Software	Microsoft/Windows/CurrentVersio	n\Group Policy\Scripts\Startu	p						
HKLM\Software	Microsoft/Windows/CurrentVersio	n\Group Policy\Scripts\Startu	p						
HKCU\Software	Microsoft/Windows/CurrentVersio	n\Group Policy\Scripts\Logor	ı						
HKLM\Software	Microsoft/Windows/CurrentVersio	n\Group Policy\Scripts\Logor	ı						
HKCU\Software	Microsoft/Windows/CurrentVersio	n\Group Policy\Scripts\Logof	F						
HKLM\Software	Microsoft/Windows/CurrentVersio	n\Group Policy\Scripts\Logof	f						
HKCU\Software	Microsoft/Windows/CurrentVersio	n\Group Policy\Scripts\Shutd	own						
HKLM\Software	Microsoft/Windows/CurrentVersio	n\Group Policy\Scripts\Shutd	own						
HKCU\Software	Microsoft \Windows \Current Versio	n\Policies\System\Shell				2018	/3/7 16:23		
HKCLINSOFTWA	RE\Microsoft\Windows.NT\Current	ntVersion\Winlocon\Shell				2018	/3/7 16:23		*
•								and the second	•

图 3-36 显示键值为空的注册表条目

(5) 在 Options 菜单中其他 3 个选项分别为: Hide Microsoft Entries 表示隐藏微软 官方的注册表条目,默认不勾选; Hide Windows Entries 表示隐藏 Windows 系统程序的 自启动条目,默认勾选此选项; Hide Virus Total Clean Entries 表示隐藏清理病毒总数量 条目。

(6) Autoruns 菜单栏中的 User 菜单中列出了可以查看的属于当前用户的启动项, 用户可以在此切换用户身份,以便查看不同用户的启动项,如图 3-37 所示。



图 3-37 User 菜单内容

(7) 在 Autoruns 的 Everything 主要内容显示区域,数据分为 6 列,分别是 Autorun Entry(条目名称)、Description(条目描述)、Publisher(发布者)、Image Path(路径)、Time-stamp(创建时间)、Virus Total(病毒数量),如图 3-38 所示。

Autoruns [WIN7-PC\Admini	strator] - Sysinternals: www.sysint	ernals.com						- • ×
File Entry Options User	Help							
_ = ₩₩ × m	iter:							
KnownDLLs	Winsock Providers	Print Monitors 3	LSA Providers	Netwo	rk Providers	WMI .	· Sidebar Gadgets	Office
Everything Logon	2 . Explorer Internet Explor	er 📓 Scheduled Tasks	Services	Drivers	200 Codecs	Boot Execute	Image Hijacks	AppInit
Autorun Entry	Description	Publisher	Image F	Path		Timestamp	VirusT	Total
HKLM\SYSTEM\CurrentControl	Set\Control\SafeBoot\AlternateShell					2009/7/14 12:37		
Cmd.exe	Windows 命令处理程序	Microsoft Corporation	c:\windo	ws\system32\c	md.exe	2010/11/20 17:00		E
HKLM\SOFTWARE\Microsoft\	Windows\CurrentVersion\Run					2018/8/21 10:29		
Safetray	安全防护中心模块		c:\progra	am files\safe\sa	fem	2018/4/17 0:43		
HKLM\SOFTWARE\Microsoft\	Active Setup \Installed Components					2011/4/12 15:18		
Browser Customizations	Windows 主进程 (Rundll32)	Microsoft Corporation	c:\windo	ws\system32\n	undli32.exe	2009/7/14 7:41		
Microsoft Windows	Windows Mail	Microsoft Corporation	c:\progra	am files\window	s mail\winmai	2009/7/14 7:42		
V n/a	Windows 主进程 (Rundll32)	Microsoft Corporation	c:\windo	ws\system32\n	undll32.exe	2009/7/14 7:41		
Themes Setup	Microsoft(C) 注册服务器	Microsoft Corporation	c:\windo	ws\system32\n	egsvr32.exe	2009/7/14 7:58		
🔽 💆 Windows Desktop Upda	te Microsoft(C)注册服务器	Microsoft Corporation	c:\windo	ws\system32\n	egsvr32.exe	2009/7/14 7:58		
HKLM\Software\Classes*\She	IEx\ContextMenuHandlers					2018/8/21 14:05		
SafeExt	安全卫士 系统扩展模块		c:\progra	am files\safe\uti	s\s	2016/10/20 12:08		
SoftMgrExt	软件管家		c:\progra	am files\safe\so	ftmg	2015/5/27 15:47		
HKLM\Software\Classes\Direct	ory\ShellEx\ContextMenuHandlers					2018/8/21 10:29		
SafeExt	安全卫士 系统扩展模块		c:\progra	am files\safe\uti	s\s	2016/10/20 12:08		
HKLM\Software\Classes\Direct	ory\Background\ShellEx\ContextMenuH	andlers				2018/8/21 14:05		
Gadgets	边栏拖动目标	Microsoft Corporation	c:\progra	am files\window	s sidebar\sb	2009/7/14 9:09		
SoftMgrExt	软件管家		c:\progra	am files\safe\so	ftmg	2015/5/27 15:47		
HKLM\Software\Classes\Folder	<pre> \ShellEx\ContextMenuHandlers </pre>					2018/8/21 10:29		
SafeExt	安全卫士 系统扩展模块		c:\progra	am files\safe\uti	s\s	2016/10/20 12:08		
HKLM\Software\Microsoft\Win	dows\CurrentVersion\Explorer\ShellIcon(OverlayIdentifiers				2018/8/21 10:29		
UDiskGuard Ico	安全卫士 木马防火墙横块		c./oroar	am files\safe\sa	fem	2016/4/15 16:44		*
								+

图 3-38 Everything 内容显示区域

(8) Everything 内容显示区域中的淡紫色行(行中包含背景色)表示注册表中的该键的路径,紫色行下面的是子键,是具体的自启动条目信息和路径。Autoruns 基于注册表的键进行类别划分,比如最上面的三行是用户登录时自启动的项,和 Logon 选项卡的内容相同,如图 3-39 和图 3-40 所示。

The Australian D		a Contata a la constata a						
Autoruns [V	VIN/-PC\Administrato	or] - Sysinternais: www.sysinter	nals.com					
File Entry (Options User Help							
	🗙 Filter:							
KnownDL	Ls 🔐 Winlogon	Winsock Providers	Print Monitors	SA Providers	twork Providers	WMI	Sidebar Gadgets	Office
Everything	Logon 2. 8	Explorer Internet Explorer	Scheduled Tasks	Services Drivers	Codecs	Boot Execute	Image Hijacks	AppInit
Autorun Entry	De	escription	Publisher	Image Path		Timestamp	VirusT	otal
HKLM\SYS	TEM\CurrentControlSet\Co	ontrol\SafeBoot\AlternateShell				2009/7/14 12:37		
Cmd.	exe Win	ndows 命令处理程序	Microsoft Corporation	c:\windows\system3	2\cmd.exe	2010/11/20 17:00		E
HKLM\SOF	TWARE\Microsoft\Windov	ws\CurrentVersion\Run				2018/8/21 10:29		
Safe	tray	安全防护中心模块		c:\program files\safe	\safem	2018/4/17 0:43		
HKLM\SOF	TWARE\Microsoft\Active 3	Setup Installed Components				2011/4/12 15:18		
Brow	rser Customizations Win	ndows 主进程 (Rundll32)	Microsoft Corporation	c:\windows\system3	2\rundll32.exe	2009/7/14 7:41		
Micro	osoft Windows Win	ndows Mail	Microsoft Corporation	c:\program files\wind	ows mail\winmai	2009/7/14 7:42		
📝 🔜 n/a	Win	ndows 主进程 (Rundll32)	Microsoft Corporation	c:\windows\system3	2\rundll32.exe	2009/7/14 7:41		
There	nes Setup Micr	crosoft(C) 注册服务器	Microsoft Corporation	c:\windows\system3	2\regsvr32.exe	2009/7/14 7:58		
V 💆 Wind	dows Desktop Update Micr	crosoft(C) 注册服务器	Microsoft Corporation	c:\windows\system3	2\regsvr32.exe	2009/7/14 7:58		
HKLM\Softv	vare\Classes*\ShellEx\Co	ontextMenuHandlers				2018/8/21 14:05		
Safe	Ext	安全卫士 系统扩展模块		c:\program files\safe	\utils\s	2016/10/20 12:08		
Soft!	MgrExt	软件管家		c:\program files\safe	\softmg	2015/5/27 15:47		
HKLM\Softv	ware\Classes\Directory\Sh	nellEx\ContextMenuHandlers				2018/8/21 10:29		
I Safe	Ext	安全卫士 系统扩展模块		c:\program files\safe	∖utils\s	2016/10/20 12:08		
HKLM\Softv	ware\Classes\Directory\Ba	ackground\ShellEx\ContextMenuHan	dlers			2018/8/21 14:05		
Gadg	gets 边相	栏拖动目标	Microsoft Corporation	c:\program files\wind	ows sidebar\sb	2009/7/14 9:09		
Soft!	MgrExt	软件管家		c:\program files\safe	\softmg	2015/5/27 15:47		
HKLM\Softy	vare\Classes\Folder\ShellE	Ex\ContextMenuHandlers				2018/8/21 10:29		
Safe	Ext	安全卫士 系统扩展模块		c:\program files\safe	\utils\s	2016/10/20 12:08		
HKLM\Softy	ware\Microsoft\Windows\C	Current Version \Explorer \Shell IconOv	erlayIdentifiers			2018/8/21 10:29		
	UDiskGuard Ico	安全卫士 木马防火墙模块		c:\orogram files\safe	\safem	2016/4/15 16:44		
•			III					•

图 3-39 Everything 选项卡内容

(9) 单击终端安全管理系统"安全防护中心模块",当需要禁用此启动项时取消该条 目前面的勾选即可,如图 3-41 所示。

Autoruns [WIN7-PC\Administrator] - Sysinternals: www.sysinter	rnals.com			-	×
File Entry Options User Help					
2 🐴 🖬 🗶 🖐 Filter:					
KnownDLLs Winlogon Winsock Providers	Print Monitors	SS LSA Providers SS Network Providers	WMI 🧱	Sidebar Gadgets	Office
Everything Logon z. Explorer Internet Explored	C Scheduled Task	s Services Services Codecs	Boot Execute	Image Hijacks	AppInit
Autorun Entry Description	Publisher	Image Path	Timestamp	VirusT	otal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			2009/7/14 12:37		
☑ [■] cmd.exe Windows 命令处理程序	Microsoft Corporation	c:\windows\system32\cmd.exe	2010/11/20 17:00		
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			2018/8/21 10:29		
☑ Safetray 安全防护中心模块		c:\program files\safe\safem	2018/4/17 0:43		
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			2011/4/12 15:18		
Browser Customizations Windows 主进程 (Rundll 32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	2009/7/14 7:41		
Vindows Windows Mail	Microsoft Corporation	c:\program files\windows mail\winmai	. 2009/7/14 7:42		
III 🔜 n/a Windows 主进程 (Rundli 32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	2009/7/14 7:41		
☑ Themes Setup Microsoft(C) 注册服务器	Microsoft Corporation	c:\windows\system32\regsvr32.exe	2009/7/14 7:58		
☑ 型 Windows Desktop Update Microsoft(C) 注册服务器	Microsoft Corporation	c:\windows\system32\regsvr32.exe	2009/7/14 7:58		

图 3-40 Logon 选项卡内容

File Entry Op	tions User H	ielp								
a 2 #	Filt	er:								
KnownDLLs	Winlog	on neg	Winsock Providers	Print Monitors	LSA Providers	Metwo	ork Providers	WMI	Sidebar Gadgets	Mi Office
Everything	Logon	2 . Explorer	Internet Explorer		Services	Drivers	Eug Codecs	Boot Exe	cute Image Hijacks	AppInit
Autorun Entry		Description		Publisher	Image	Path		Timestamp	VirusT	otal 🔺
HKLM\SYSTE	M\CurrentControlS	et\Control\Safe	Boot \Alternate Shell					2009/7/14 12:37		
Crnd.ex	e	Windows 命令	〉处理程序	Microsoft Corporation	c:\wind	ows\system32\a	md.exe	2010/11/20 17:00	0	E
HKLM\SOFTV	VARE\Microsoft\W	indows\Current	Version\Run					2018/8/21 10:29		
Safetra		安全	:防护中心模块		c:\prog	am files\\safe\si	afem	2018/4/17 0:43		
HKLM\SOFTV	VARE\Microsoft\Ad	tive Setup\Inst	alled Components					2011/4/12 15:18		
Browse	r Customizations	Windows 主逆	主程 (Rundll32)	Microsoft Corporation	c:\wind	ows\system32\r	undll32.exe	2009/7/14 7:41		
Microso	oft Windows	Windows Mail		Microsoft Corporation	c:\prog	am files\window	/s mail\winmai	2009/7/14 7:42		
n/a		Windows 主法	主程 (Rundli32)	Microsoft Corporation	c:\wind	ows\system32\r	undli32.exe	2009/7/14 7:41		
Theme	s Setup	Microsoft(C)	E册服务器	Microsoft Corporation	c:\wind	ows\system32\r	egsvr32.exe	2009/7/14 7:58		
V 🖾 Window	vs Desktop Update	Microsoft(C)	E册服务器	Microsoft Corporation	c:\wind	ows\system32\r	egsvr32.exe	2009/7/14 7:58		
HKLM\.Softwa	re\Classes*\ShellE	x\ContextMen	Handlers					2018/8/21 14:05		
SafeEx	t	安全卫士	系统扩展模块		c:\prog	am files\safe\ut	ils\s	2016/10/20 12:00	8	
Soft Mg	rExt	软件管家			c:\prog	am files\safe\so	ftmg	2015/5/27 15:47		
HKLM\Softwa	re\Classes\Director	y\ShellEx\Cont	extMenuHandlers					2018/8/21 10:29		
SafeEx	t	安全卫士	系统扩展模块		c:\prog	am files\safe\ut	ils\s	2016/10/20 12:00	8	
HKLM\Softwa	re\Classes\Director	y\Background\	ShellEx\ContextMenuHar	ders				2018/8/21 14:05		
Gadget	s	边栏拖动目标	7	Microsoft Corporation	c:\prog	am files\window	/s sidebar\sb	2009/7/14 9:09		
Soft Mg	rExt	软件管家			c:\prog	am files\safe\so	ftmg	2015/5/27 15:47		
HKLM\Softwa	re\Classes\Folder\	ShellEx\Context	MenuHandlers					2018/8/21 10:29		
SafeEx	t	安全卫士	系统扩展模块		c:\prog	am files\safe\ut	ils\s	2016/10/20 12:0	8	
HKLM\Softwa	re\Microsoft\Windo	ws\CurrentVers	sion\Explorer\ShellIconOv	erlayIdentifiers				2018/8/21 10:29		
	UDiskGuard Ico	安全卫士	木马防火搞模块		c./uuu	am files\safe\sa	fem	2016/4/15 16:44		
•										+
itray	.exe	Siz	e: 428 K							
天調	医全防护中心槽	块 Tim	e: 2018/4/17 0:43							
		Ver	sion: 8.0.0.1097							
"C+\Pro	ram Files\Safe\safe	emon\Trav ev	e" /start							
0.410	grown new pare par	chioritridy.ex	c jour c							

图 3-41 选中条目

(10) 右击选中终端安全管理系统"安全防护中心模块",会弹出可操作菜单,Delete 是删除此启动条目,无法恢复;Copy 会复制此条数据,包括 Autorun Entry、Description、 Publisher、Image Path、Timestamp 和 Virus Total,如图 3-42 所示。

Delete	Ctrl+D
Сору	Ctrl+C
Jump to Entry	
Jump to Image	
Verify Image	
Check VirusTotal	
Process Explorer	
Search Online	Ctrl+M
Find	Ctrl+F
Properties	Alt+Enter

图 3-42 条目操作菜单

(11) Jump to Entry 会跳转至该自启动条目在注册表中的键的位置,如图 3-43 所示。

1 注册表编辑	up. In					
文件(F) 编辑	(E) 查看(V)	收藏夹(A)	帮助(H)			
		Hints 🔺	名称	美型	数据	
	Þ - 🏬	Home(@)(默认)	REG_SZ	(数值未设置)	
		HotSta	ab Safetray	REG_SZ	"C:\Program Files\Safe\safemon\tray.exe" /start	
	P - 🛄	IME				
	P - ₩	Installe				
	P - 🛄	Interne				
	P	MCI				
		Media				
		MCCLL				
		NetCa:				
		OFMIr				
		OOBE				
		Optim				
	Þ-11	Parent				
		Persor				
	Þ-1	PhotoF				
	Þ - 📗	PnPSys				
	Þ - 📗	Policie				
		Previe				
	Þ - 📗	Proper				
	Þ - 📗	Reliabi				
	Þ 🃗	Renam				
		Run				
<		RunOn ▼				
, 计算机\HKEY_L	OCAL_MAC	HINE\SOFT	VARE\Microsoft\Win	dows\CurrentVersion	\Run	

图 3-43 Jump to Entry

(12) Jump to Image 会跳转至该启动条目的执行文件位置,如图 3-44 所示。

组织 ▼ 🗐 打开	新建文件夹			-	
 ☆ 收藏夹 ↓ 下载 ■ 桌面 ③ 最近访问的位置 	名称 mpspopwnd.dii PayInsure procmon.dli realpro	修改日期 2016/3/22 10:33 2018/6/19 15:01 2018/5/22 16:33 2018/6/21 11:50	类型 应用程序 应用程序扩展 应用程序扩展	大小 1,503 ND 1,469 KB 485 KB 461 KB	
 □ 库 ■ 砌坂 ■ 図片 ⊇ 文档 ↓ 音乐 	RealproEx SafeCamera.tpi safemonpro.tpi sclog sctblist SelfProtection.sys	2018/6/19 20:53 2018/6/21 11:50 2018/6/21 11:50 2018/6/21 11:50 2018/6/21 11:50 2018/5/22 16:33	应用程序 TPI 文件 TPI 文件 应用程序 应用程序 系统文日 君	745 KB 386 KB 1,670 KB 421 KB 406 KB 192 KB	
■ 计算机	selfprotection_win10 SelfProtection_win10.sys settingcenter SPTool Toasts	2018/5/1/ 12:19 2018/5/22 16:33 2018/6/21 17:37 2018/5/18 20:03 2018/6/19 20:53 2018/5/22 16:33	安全自录 系統文件 应用程序 应用程序 应用程序	10 KB 200 KB 697 KB 172 KB 144 KB	

图 3-44 Jump to Image

(13) Verify Image 可以校验该自启动条目的执行文件的签名,进行真实性验证,验证通过后会在 Publisher 字段添加(Verified)字段,如图 3-45 所示。