第3章 资产日志管理与设置

网络系统中的日志有不同的采集对象以及不同的采集方式，日志形式也多种多样，故需要进行归一化处理，为其他模块的计算分析奠定基础。

3.1 日志审计与分析系统资产录入实验

【实验目的】

日志审计与分析系统将其他设备作为资产录入本系统，然后对这些设备的日志进行审计与分析，本实验实现对当前资产组的添加、修改、删除，同时对资产组中的资产进行录入。

【知识点】

资产、资产组、资产录入。

【实验场景】

A公司的日志审计与分析设备由安全运维工程师小王负责。由于公司资产较多，小王想对资产进行分类分组管理。请思考应如何操作。

【实验原理】

日志审计与分析系统的资产组树可以完成对当前资产组的添加、修改、删除等操作，同时还可以对资产组中已经存在的资产进行统计和查看，通过资产的名称、IP等信息查看资产，统计资产的其他属性。

【实验设备】

- 安全设备：日志审计与分析设备1台。

【实验拓扑】

日志审计与分析系统资产录入实验拓扑图如图3-1所示。

【实验思路】

(1) 以管理员admin用户的身份登录日志审计与分析系统。

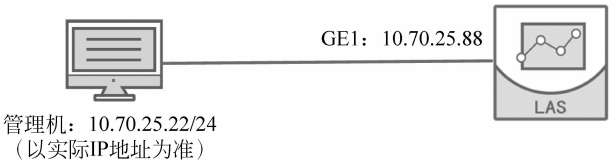

图 3-1　日志审计与分析系统资产录入实验拓扑图

（2）创建新的资产组“服务器”。

（3）在资产组中录入资产。

（4）对当前资产组中的资产进行统计和查看。

【实验步骤】

（1）在管理机中打开浏览器，在地址栏中输入日志审计与分析产品的 IP 地址“https://10.70.25.88”（以实际 IP 地址为准），打开平台登录界面。由于此网址的证书未经过认证，会显示“此站点不安全”，单击“详细信息”按钮。

（2）在“详细信息”的下面，单击“转到此网页”按钮，这样在不关闭浏览器的情况下可以正常访问此网址。

（3）使用管理员用户名/密码“admin/!1fw@2soc#3vpn”登录日志审计与分析系统。

（4）登录后，需要修改 admin 用户的密码，本实验没有修改密码的必要，所以“原始密码”“新密码”“确认新密码”都输入“!1fw@2soc#3vpn”，单击“确定”按钮。

（5）登录后，将日志审计与分析系统的网址加入浏览器兼容性视图中，以保证网站中的内容可以正确显示，单击浏览器的“设置”→“兼容性视图设置”，进入“兼容性视图设置”界面。

（6）进入“兼容性视图设置”界面后，在“添加此网站”下面输入设备地址“192.168.1.60”，然后单击“添加”按钮。

（7）完成兼容性设置后，关闭“兼容性视图设置”界面，进入日志审计与分析系统界面，选择“资产”命令，进入资产模块，如图 3-2 所示。

图 3-2　进入资产模块

（8）首先进行资产分组，创建新的资产组，选中“资产对象”，单击“添加”按钮，如图 3-3 所示。

（9）输入新资产组名称为“服务器”，单击“确定”按钮，如图 3-4 所示。

（10）同时也可以对已添加的资产组进行修改、删除、导入和导出等操作，根据需要进行，本实验不再演示，如图 3-5 所示。

图 3-3　添加资产组

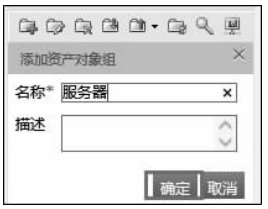

图 3-4　编辑资产组信息

图 3-5　编辑资产组信息

（11）接下来进行资产录入，单击新创建的资产组“服务器”，再单击“添加”按钮，进行资产添加，如图 3-6 所示。

图 3-6　添加资产

（12）编辑资产信息，“设备名称”输入“Windows 服务器”，“设备 IP”输入“192.168.1.70”，“子网掩码”输入“255.255.0.0”，“业务关键度”输入 3.0；选择“设备类型”为“服务器”，“设备型号”为 Windows。本实验中给出的设备 IP、子网掩码等信息仅供参考，请根据实际情况填写，单击“确定”按钮，如图 3-7 所示。

（13）完成添加后，可以在设备列表中看到新录入的资产“Windows 服务器”，如图 3-8 所示。

（14）若要修改资产信息，选中资产地址，单击“修改”命令，重新编辑资产信息。同理，也可以进行删除、移动、导入、导出等操作，如图 3-9 所示。

【实验预期】

（1）可以看到新添加的分组“服务器”以及新添加的资产“Windows 服务器”。

（2）对创建的资产“Windows 服务器”通过名称进行查询，并查看设备统计。

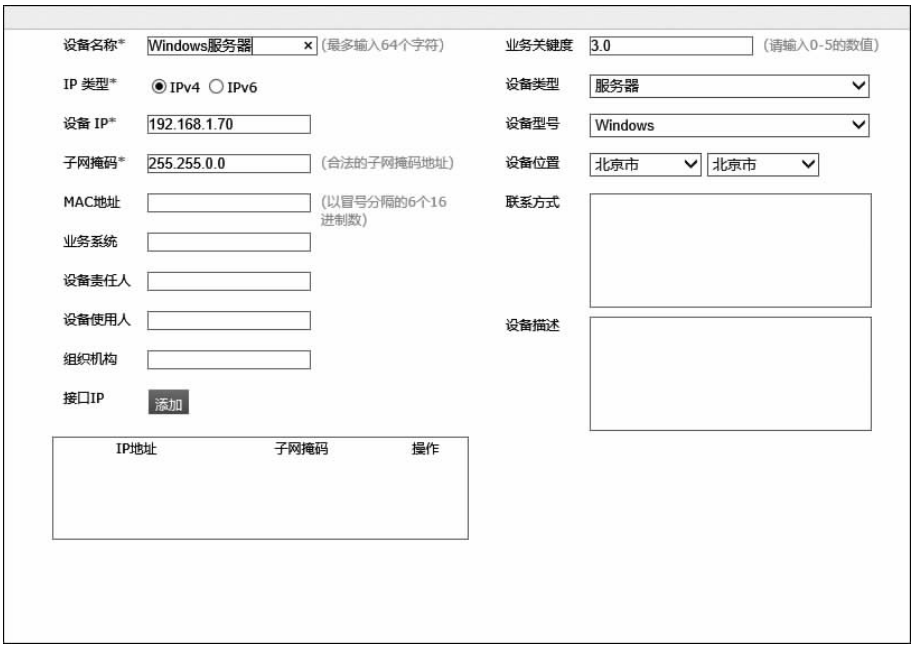

图 3-7　编辑资产信息

图 3-8　资产组列表

图 3-9　修改资产信息

【实验结果】

(1) 在资产对象的资产组树中显示添加成功的资产组“服务器”,如图 3-10 所示。

(2) 在设备列表中可看到新添加的资产“Windows 服务器”,如图 3-11 所示。

(3) 单击资产组中的“查询”,通过名称查找已有资产“Windows 服务器”,单击“确定”按钮,如图 3-12 所示。

(4) 成功查到已有资产“Windows 服务器”,如图 3-13 所示。

(5) 管理员在资产树中设备统计中可以查看资产信息,如图 3-14 所示。

图 3-10　创建新资产组成功

图 3-11　添加资产成功

图 3-12　查询资产

图 3-13　查询成功

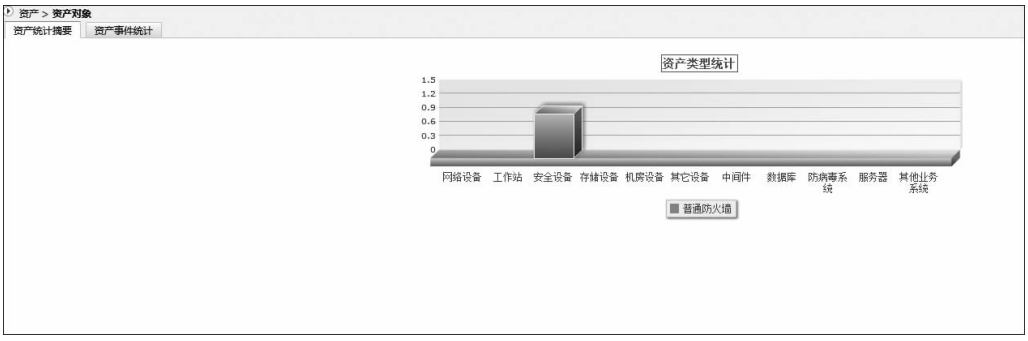

图 3-14　设备统计

【实验思考】

(1) 如果需要修改资产的 IP 信息，应该如何做？

(2) 在资产中如何设置接口信息？

3.2 日志审计与分析系统资产批量导入导出与属性设置实验

【实验目的】

本实验完成对日志审计与分析系统中资产的批量导入、导出以及属性设置。

【知识点】

资产导入、资产导出、XLS 格式。

【实验场景】

A 公司的日志审计与分析设备由安全运维工程师小王负责。公司需要将一批资产导入到日志审计与分析系统中，并对这些资产进行安全等级划分等操作。请思考应如何操作能够实现批量将这些资产导入到设备中，以及如何将资产信息导出设备。

【实验原理】

在日志审计与分析系统中，用户可以在资产对象安全域列表中，单击“导入”，并在资产导入列表中，选择要导入的资产信息文件，确定导入策略，完成资产的批量导入。导出资产时只须选择资产信息导出路径，即可完成资产导出。资产属性的设置需要将“资产”→“资产属性”中的属性标签与资产相关联。

【实验设备】

- 安全设备：日志审计与分析设备 1 台。

【实验拓扑】

日志审计与分析系统资产批量导入导出与属性设置实验拓扑图如图 3-15 所示。

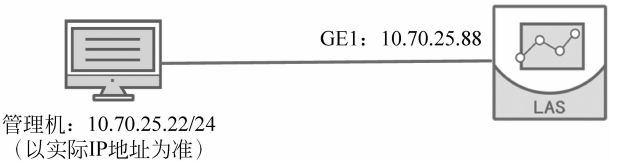

图 3-15　日志审计与分析系统资产批量导入导出与属性设置实验拓扑图

【实验思路】

（1）以管理员 admin 的身份登录日志审计与分析系统。

（2）依次单击“资产”→“资产列表”，进行资产信息批量导入导出。

（3）设置资产属性。

【实验步骤】

（1）在管理机中打开浏览器，在地址栏中输入日志审计与分析产品的 IP 地址“https://10.70.25.88”（以实际 IP 地址为准），打开平台登录界面。由于此网址的证书未经过认证，会显示“此站点不安全”，单击“详细信息”按钮。

（2）在“详细信息”的下面，单击“转到此网页”按钮，这样在不关闭浏览器的情况下可以正常访问此网址。

（3）使用管理员用户名/密码“admin/!1fw@2soc#3vpn”登录日志审计与分析系统。

（4）登录后，需要修改 admin 用户的密码，本实验没有修改密码的必要，所以“原始密码”“新密码”“确认新密码”都输入“!1fw@2soc#3vpn”，单击“确定”按钮。

（5）登录后，将日志审计与分析系统的网址加入浏览器兼容性视图中，以保证网站中的内容可以正确显示，单击浏览器的“设置”→“兼容性视图设置”，进入“兼容性视图设置”界面。

（6）进入“兼容性视图设置”界面后，在“添加此网站”下面输入设备地址“10.70.25.88”，然后单击“添加”按钮。

（7）完成兼容性设置后，关闭“兼容性视图设置”界面，进入日志审计与分析系统界面，单击“资产”，进入资产模块，如图 3-16 所示。

（8）依次单击“资产”→“资产对象”，首先新建资产组，单击“新建”按钮，如图 3-17 所示。

（9）名称输入“服务器”，单击“确定”按钮，如图 3-18 所示。

（10）在资产组“服务器”中进行资产添加，单击“添加”按钮，如图 3-19 所示。

（11）编辑资产信息，“设备名称”输入“Windows 服务器”，“设备 IP”输入“192.168.0.104”，“子网掩码”输入“255.255.0.0”，“业务关键度”输入 3.0；选择“设备类型”为“服务器”，“设备型号”为 Windows。本实验中给出的设备 IP、子网掩码等信息仅供参考，请根据实际情况填写，单击“确定”按钮，如图 3-20 所示。

图 3-16　进入“资产”模块

图 3-17　新建资产组

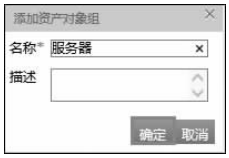

图 3-18　新建资产组

图 3-19　添加资产

图 3-20　编辑 Windows 服务器资产信息

（12）完成“Windows 服务器”添加后，继续进行“Linux 服务器”的添加，重复步骤（10）和（11），编辑资产信息，“设备名称”输入“Linux 服务器”，“设备 IP”输入“192.168.0.105”，“子网掩码”输入“255.255.0.0”，“业务关键度”输入 3.0；选择“设备类型”为“服务器”，“设备型号”为 Linux。本实验中给出的设备 IP、子网掩码等信息仅供参考，请根据实际情况填写，单击“确定”按钮，如图 3-21 所示。

图 3-21　编辑 Linux 服务器资产信息

（13）批量导出资产时，将资产批量选中，单击“导出”按钮，选择导出格式，本系统能够以三种格式导出资产，分别是 xml、csv 和 xls。本实验中选择 xls 格式进行导出，便于导出后查看资产信息，如图 3-22 所示。

图 3-22　导出 XLS 格式的资产信息

（14）单击“导出”按钮后，选择文件的保存路径，本实验中，将文件存放至管理机桌面。首先单击“保存”按钮，然后选择保存文件至桌面，如图 3-23 所示。

（15）完成资产导出后进行资产导入，新建“防火墙”资产组，单击“新建”按钮，并输入资产组名称为“防火墙”，如图 3-24 所示。

图 3-23　保存导出资产

图 3-24　新建防火墙资产组

（16）在批量导入资产信息时，必须符合日志系统要求的格式才可以被识别，因此需要按照模板来填写资产信息，单击“导入”按钮，单击“下载”按钮进行模板的下载，并将其存放于管理机桌面，如图 3-25 所示。

图 3-25　下载导入模板

（17）打开刚刚下载的模板文件，按照模板输入“资产信息”，需要填写的有“设备名称”“设备 IP”“子网掩码”“业务关键度”“设备类型”“设备型号”“设备位置”等信息，按照图 3-26 进行填写，填写完毕后，以 xls 格式另存至管理机桌面。

A	B	C	D	E	F	G	H	I	J	K	L	M	N
设备名称	设备IP	子网掩码	MAC地址	业务关键度	设备类型	设备型号	设备位置	联系方式	设备描述	业务系统	设备责任人	设备使用人	组织机构
360防火墙	192.168.1.50	255.255.255.0		0.0	安全设备	普通防火墙	北京市:北京市						
360防火墙2	192.168.2.50	255.255.255.0		0.0	安全设备	普通防火墙	北京市:北京市						
360防火墙3	192.168.3.50	255.255.255.0		0.0	安全设备	普通防火墙	北京市:北京市						

图 3-26　填写资产导入文件

（18）单击“导入”按钮后，选择导入的资产信息文件以及导入方式，本系统提供两种导入方式，分别是“增量导入”和“覆盖导入”，本实验中选择“增量导入”。单击“浏览”按钮，并选择存放在管理机桌面的资产文件“assetImportTemple. xls”，单击“确定”按钮，完成资产批量导入，如图 3-27 所示。

图 3-27　导入资产

（19）单击“资产属性”，进入资产属性管理界面，可以进行资产属性的添加、修改、删除等操作，如图 3-28 所示。

图 3-28　资产属性管理

【实验预期】

（1）导出资产文件成功。

（2）导入资产文件成功。

（3）查看新添加的资产属性，关联资产属性和相关资产。

【实验结果】

（1）导出资产文件成功，打开本实验中导出资产文件 asset. xl，打开该文件，可以查看导出资产的相关信息，如图 3-29 所示。

A	B	C	D	E	F	G	H	
设备名称	设备IP	子网掩码	MAC地址	业务关键度	设备类型	设备型号	设备位置	联
Windows服	192.168.0.	255.255.0.		3.0	服务器	Windows	北京市:北京	
Linux服务器	192.168.0.	255.255.0.		0.0	服务器	Linux	北京市:北京	

图 3-29　导出资产成功

（2）导入资产文件成功，可以在“资产”→“资产对象”中的资产列表中找到刚刚导入的资产“防火墙”“防火墙 2”以及“防火墙 3”，证明导入成功，如图 3-30 所示。

图 3-30　导入资产文件成功

（3）关联资产属性与资产，首先关联“安全等级”，依次单击“安全等级”→“中”，单击“添加”按钮，如图 3-31 所示。

图 3-31　关联资产属性

（4）选中需要关联的资产“防火墙”，单击“确定”按钮，如图 3-32 所示。

图 3-32　选中关联资产

（5）添加完成后，可以在“资产属性”→“安全等级”→“中”里面找到关联的设备“防火墙”，如图 3-33 所示。

图 3-33　查询资产

（6）当需要删除某一资产与资产属性的关联时，在该资产属性分组中找到该资产，选中后单击“删除”按钮，如图 3-34 所示。

图 3-34　查询资产

（7）同理，也可将其他属性与设备相关联，便于更加详细地描述资产，解决实验场景中的问题。

【实验思考】

（1）同一个资产设备能否同时关联一个资产属性组中的不同属性？

（2）为什么要规范几种资产文件的格式？

第4章 系统日志采集配置

为了防止恶意入侵给网络造成破坏，造成资源的丢失，网络管理人员需要能够准确、及时地了解整个网络的当前状态及未来安全趋势，及时发现攻击和危害行为，并进行应急响应，以便对网络的安全设置和资源配置做出合理的应急策略，达到事前预防、纵深防御的目的。网络安全态势评估和预测越来越受到人们的关注，成为网络安全管理领域研究中的热点问题，而关联分析则是快速定位故障和入侵的一个有效手段。

关联分析又称关联挖掘，指在关系数据或其他信息载体中，查找存在于对象集合之间的关联、相关性或因果结构，是一种在大型数据库中发现变量之间关系的方法。关联的含义是将所有系统中的事件以统一格式综合到一起进行观察。关联技术不但在商业领域被广泛使用，在医疗、保险、网络安全和电信行业等领域也得到了有效的应用。

4.1 日志审计与分析系统网络设备日志采集实验

【实验目的】

日志审计与分析系统提供日志采集功能，本实验通过 winbox 远程控制 MikroTik 路由器实现路由器的日志转发，将日志收集到日志审计与分析系统中。

【知识点】

日志收集、网络设备、路由器。

【实验场景】

A 公司的日志审计与分析系统由安全运维工程师小王负责。目前，公司要求小王利用日志审计与分析系统监控网络中的路由器的日志，以便及时发现和分析处理问题。请思考应如何实现。

【实验原理】

日志审计与分析系统能够通过多种方式全面采集网络中各种设备、应用和系统的日志，确保用户能够收集并审计必需的日志信息。RouterOS 路由系统可利用 winbox 控制台对其进行控制，通过 winbox 远程控制并修改 RouterOS 的日志参数，可将路由器的日志信息发送至日志审计与分析设备中，依次单击“资产”→“资产日志”，可查看对应的资产

日志管理信息，此外，依次单击“事件”→“实时监视”→“接收的外部事件”，可查看接收到的路由器的日志信息。

【实验设备】

- 安全设备：日志审计与分析设备 1 台。
- 主机终端：Windows 主机 1 台。
- 网络设备：路由器 1 台。

【实验拓扑】

日志审计与分析系统网络设备日志采集实验拓扑图如图 4-1 所示。

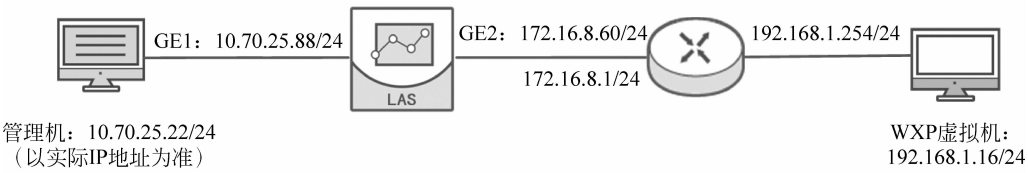

图 4-1　日志审计与分析系统网络设备日志采集实验拓扑图

【实验思路】

（1）在管理机端使用 Xshell 进入日志审计与分析系统后台，配置系统路由信息。

（2）以管理员 admin 用户的身份登录日志审计与分析系统。

（3）登录 Windows 系统，在 winbox 中进行路由器日志远程配置。

（4）修改路由器设置。

（5）在日志审计与分析系统端查看日志收集是否成功。

【实验步骤】

（1）在管理机端单击 Xshell 图标，打开 Xshell。

（2）在会话框中单击“新建”按钮，创建新的会话。

（3）在“主机”栏中输入日志审计与分析系统 GE1 接口的 IP 地址“10.70.25.88”（以实际 IP 地址为准），其他设置保持不变，单击“确定”按钮。

（4）新建的会话会在“所有会话”中显示，选中“新建会话”，单击“连接”按钮。

（5）单击“一次性接受”按钮。

（6）在“请输入登录的用户名”一栏中输入用户名 admin，单击“确定”按钮。

（7）在“密码”栏中输入密码“@1fw＃2soc＄3vpn”，单击“确定”按钮。

（8）成功登录日志审计与分析系统后台。

（9）输入命令“secfox -e eth1-p 172.16.8.60 -m 255.255.255.0”（以实际 IP 地址为准），设置日志审计与分析系统 GE2 接口的 IP 地址。其中，“172.16.8.60”是 GE2 口的 IP 地址，“255.255.255.0”是 GE2 口的子网掩码。按 Enter 键，出现“modify ip ...”，说明

接口信息配置成功。

(10) 打开浏览器,在地址栏中输入日志审计与分析系统的 IP 地址“https://10.70.25.88”(以实际 IP 地址为准),单击“继续浏览此网站”,打开平台登录界面。

(11) 输入管理员用户名/密码“admin/!1fw@2soc#3vpn”,单击“登录”按钮,登录日志审计与分析系统。

(12) 系统设置的密码有效期为 7 天,当登录系统后收到更改密码提示时,单击“确定”按钮,更改系统密码。

(13) 在“原始密码”一栏输入原始密码“!1fw@2soc#3vpn”,在“新密码”一栏输入“!1fw@2soc#3vpn”,与原始密码相同,在“确认新密码”一栏输入“!1fw@2soc#3vpn”,单击“确定”按钮。

(14) 单击浏览器中的“工具”→“兼容性视图设置”。

(15) 输入日志审计与分析系统的 IP 地址“https://10.70.25.88”(以实际 IP 地址为准),单击“添加”按钮,添加网站兼容性视图。

(16) 单击“关闭”按钮,退出设置。

(17) 进入日志审计与分析系统后,单击“系统”→“系统维护”,可看到系统“IP 地址配置 1”为“172.16.8.60”,即日志审计与分析系统 GE2 接口的 IP 地址。

(18) 将管理机时间与日志审计与分析系统时间统一。在日志审计与分析系统中,单击“系统”→“系统维护”,接着单击“时间校对设置”框中的“手动校时”选项。

(19) 单击“时间”一栏的钟表图案。

(20) 选择与管理机统一的时间(以实际时间为准)。

(21) 单击屏幕空白处,退出设置。

(22) 单击“修改时间”,完成日志审计与分析系统时间的手动修改。

(23) 修改成功后,系统会跳转至登录界面,重新输入用户名/密码“admin/!1fw@2soc#3vpn”,登录日志审计与分析系统。

(24) 重新登录后,查看系统界面右下方的时间,与管理机时间相同。

(25) 选择“con-router”,打开路由器,如图 4-2 所示。

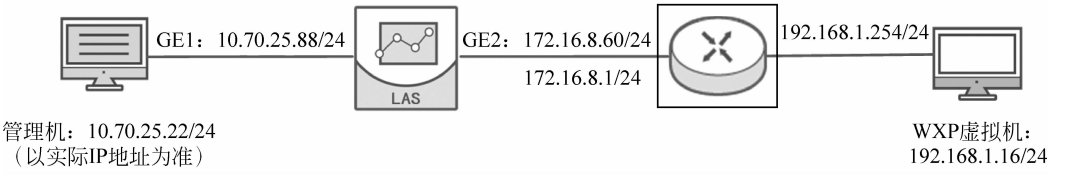

图 4-2　打开路由器

(26) 输入用户名 admin,密码为空,登录路由器,如图 4-3 所示。

图 4-3　登录路由器

(27) 输入命令“ip addr pri”,查看路由器网卡的 IP 配置。其中,与 Windows 系统相连的接口 2 的 IP 地址为“192.168.1.254”,与日志审计与分析系统相连的接口 1 的 IP 地址为“172.16.8.1”,如图 4-4 所示。

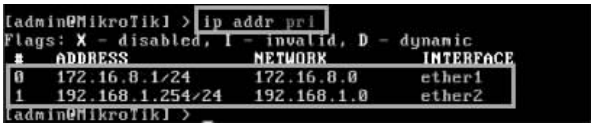

图 4-4 路由器 IP 配置

(28) 输入命令“/system ntp client”,设置时间同步,如图 4-5 所示。

图 4-5 设置时间同步

(29) 输入命令“set mode=unicast primary-ntp=210.72.145.44 secondary-ntp=210.72.145.44 enabled=yes”,设置 ntp 地址,如图 4-6 所示。

图 4-6 配置 ntp 地址

(30) 输入命令“..”,回退至上一级,如图 4-7 所示。

图 4-7 回退至上一级

(31) 输入命令“..”,回退至 system 目录下,如图 4-8 所示。

图 4-8 回退至 system 目录

(32) 输入命令“..”,回退至根目录,如图 4-9 所示。

图 4-9 回退至根目录

(33) 输入命令“/system clock set time-zone-name=Asia/Shanghai time=14:03:20 date=Apr/11/2018”(时间及日期设置以实际时间为准),其中,time-zone-name 表示时区名称,time 代表时间,date 代表日期,如图 4-10 所示。

图 4-10　设置当前时间

(34) 输入命令“/system clock pri”,查看修改后的系统时间,与管理机时间统一,如图 4-11 所示。

图 4-11　查看修改时间

(35) 选择 WXPSP3,打开 Windows 系统,如图 4-12 所示。

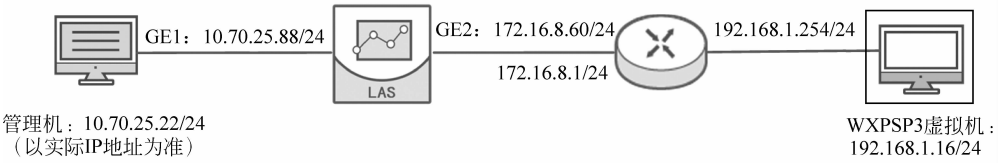

图 4-12　打开 Windows 系统

(36) 单击桌面上的“实验工具”,双击 winbox 文件夹,查看 winbox 工具。winbox 是基于 Windows 的远程管理 RouterOS 路由系统的软件,为用户提供直观方便的图形界面,如图 4-13 所示。

图 4-13　打开 winbox 文件夹

(37) 双击“winbox5. x 中文版. exe”,打开 winbox 工具,如图 4-14 所示。

图 4-14　打开 winbox 工具

(38) 在“路由地址”一栏输入路由器接口 2 的 IP 地址“192.168.1.254”(以实际 IP 地址为准),单击“连接”按钮,如图 4-15 所示。

图 4-15　winbox 远程连接路由器

(39) 单击“系统”→“日志”,打开 winbox 的日志管理,如图 4-16 所示。

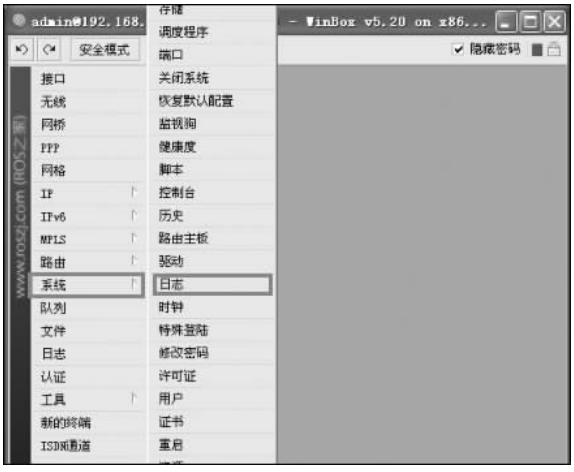

图 4-16　打开 winbox 日志管理

(40) 选择“动作”标签页，双击名称为 remote 且类型为“远程”一栏，配置远程地址，如图 4-17 所示。

图 4-17　打开日志的远程设置

(41) 在“远程地址”一栏输入日志审计与分析系统的 IP 地址“172.16.8.60”，其他配置保持默认值不变，单击“确定”按钮，如图 4-18 所示。

图 4-18　设置日志远程地址

(42) 选择“规则”标签页，双击主题为 info 一栏，如图 4-19 所示。

(43) 单击“动作”一栏的下拉选项，选择 remote，单击“确定”按钮，将 info 信息发送至日志审计与分析系统，如图 4-20 所示。

(44) 将主题为 critical、error 和 warning 对应的动作也修改为 remote，操作与 info 一